SINDICATURA DE COMPTES
DE LA COMUNITAT VALENCIANA

INFORME DE SEGUIMENT DE LES RECOMANACIONS REALITZADES EN L'INFORME D'AUDITORIA DELS CONTROLS BÀSICS DE CIBERSEGURETAT DE L'AJUNTAMENT D'ELX DE L'ANY 2019

Situació a 31 de desembre de 2021

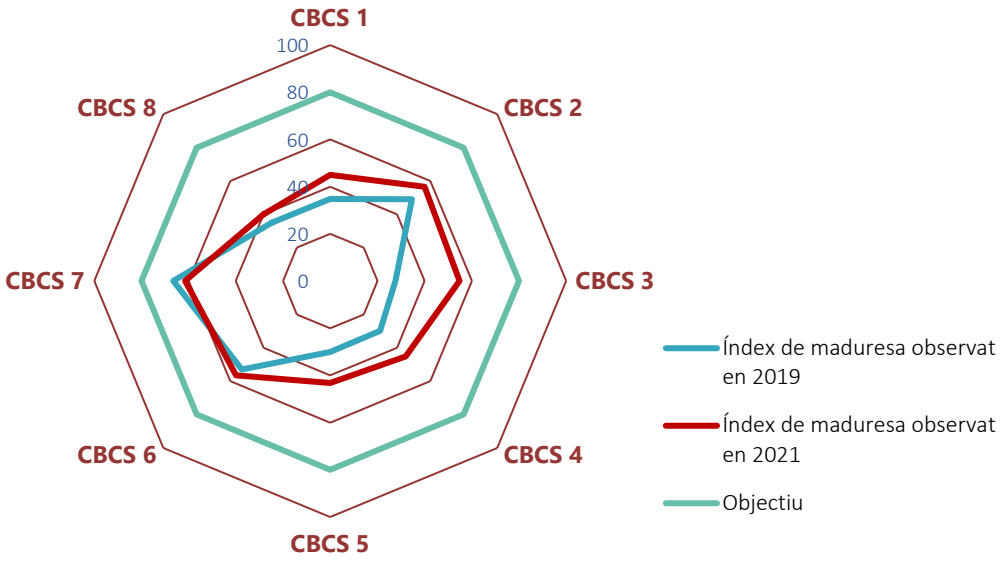
RESUM

La transformació digital que estan experimentant totes les administracions públiques i la seua interconnexió a través de complexes xarxes informàtiques les exposa de manera cada vegada més intensa a amenaces provinents del ciberespai. Això origina un increment dels riscos associats als sistemes d'informació que sustenten els serveis públics i, per tant, a la informació que manegen. De fet, les entitats locals han sigut un dels objectius més afectats per les onades recents de ciberatacs.

Atesa aquesta realitat, i en sintonia amb el seu actual pla estratègic, la Sindicatura de Comptes ha fet un treball de seguiment dels controls bàsics de ciberseguretat (CBCS) de l'Ajuntament d'Elx respecte a la situació que mostrava l'auditoria de l'any 2019.

Conclusions

Encara que s'han realitzat progressos des de la nostra auditoria anterior i s'han atés parcialment algunes de les nostres recomanacions, l'índex de maduresa general dels controls bàsics de ciberseguretat, l'objectiu dels quals seria aconseguir un 80% , mostra un valor del 50,3% (40,7% en 2019), per la qual cosa el nivell d'efectivitat en els controls analitzats continua sent insuficient i ha de millorar per a aconseguir els nivells exigits per l'Esquema Nacional de Seguretat per a la protecció dels sistemes d'informació, especialment en els controls que presenten deficiències significatives.



L'Ajuntament d'Elx no té establida una adequada governança de la ciberseguretat, situació que s'ha d'esmenar. Els òrgans de govern han d'aprovar normes i procediments en relació amb la seguretat de la informació aplicables a tota l'organització per igual. També cal que el comité de seguretat de la informació, òrgan imprescindible per a coordinar la seguretat

de la informació en l'entitat, es reunisca regularment, a fi de conéixer l'estat de la seguretat de la informació de l'Ajuntament i prendre les decisions pertinents de manera oportuna.

Així mateix, la nostra revisió també ha posat de manifest un grau de compliment molt deficient quant a l'adequació a les normes legals relacionades amb la seguretat de la informació. L'informe assenyala diversos aspectes sobre els quals s'ha d'actuar per a esmenar-los ràpidament

També hem realitzat una sèrie de recomanacions amb el propòsit de contribuir a esmenar les deficiències observades i millorar els procediments de gestió de la ciberseguretat de l'Ajuntament. Entre aquestes, aprovar formalment un procediment unificat per a la gestió de l'inventari i el control d'actius físics i de programari que reculla el procés actualment implantat i s'aplique a tots els sistemes d'informació de l'Ajuntament; aconsellem finalitzar la implantació de solucions per a restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa; elaborar i aprovar formalment un procediment per a gestió d'usuaris amb privilegis d'administració, i aprovar i implantar un procediment de configuració segura o fortificació dels sistemes que considere la seguretat per defecte i el criteri de mínima funcionalitat.

NOTA

Aquest resum pretén ajudar a comprendre els resultats del nostre informe i facilitar la tasca als lectors i als mitjans de comunicació. Recomanem llegir-lo per a conéixer el veritable abast del treball realitzat.

Informe de seguiment de les recomanacions realitzades en l'informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament d'Elx de l'any 2019

Situació a 31 de desembre de 2021

Sindicatura de Comptes
de la Comunitat Valenciana

ÍNDEX (amb hipervincles)

1. Introducció 3
2. Responsabilitats dels òrgans superiors de l'Ajuntament en relació amb els controls de ciberseguretat 4
3. Responsabilitat de la Sindicatura de Comptes 4
4. Conclusions 5
5. Recomanacions i mesures necessàries per al compliment de la legalitat 9
Apèndix 1. Metodologia aplicada 19
Apèndix 2. Situació dels controls bàsics de ciberseguretat 36
Apèndix 3. Bones pràctiques destacables 47
Acrònims i glossari de termes 50
Tràmit d'al·legacions 53
Aprovació de l'Informe 54

1. INTRODUCCIÓ

Per què realitzem aquesta auditoria

L'article 6 de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, inclou entre les seues funcions, a més de les referides al control extern de la gestió economicofinancera del sector públic valencià i dels seus comptes, les que d'acord amb l'ordenament jurídic siguen convenients per a assegurar adequadament el compliment dels principis financers, de legalitat, d'eficàcia, d'economia i de transparència, exigibles al sector públic, així com la sostenibilitat ambiental i la igualtat de gènere. D'altra banda, l'article 11 de la mateixa llei estableix que, en el desenvolupament de la seua funció fiscalitzadora, la Sindicatura de Comptes està facultada per a **verificar la seguretat i fiabilitat dels sistemes informàtics** que suporten la informació economicofinancera, comptable i de gestió.

En la guia d'auditoria GPF-OCEX 5311, "Ciberseguretat, seguretat de la informació i auditoria externa", del *Manual de fiscalització* de la Sindicatura de Comptes, es destaca la importància creixent que les qüestions relacionades amb la ciberseguretat estan adquirint en la gestió de les administracions públiques, raó per la qual els auditors públics els han de prestar cada vegada més atenció. En línia amb això, **en el Pla Estratègic de la Sindicatura de Comptes per al període 2019-2022 s'assenyala la ciberseguretat com una de les àrees d'alt risc i prioritàries per a dur a terme la tasca fiscalitzadora**.

En 2019 i 2020 la Sindicatura de Comptes va realitzar sengles auditories sobre la situació dels controls bàsics de ciberseguretat (CBCS) dels 15 ajuntaments de la Comunitat Valenciana amb una població superior a 50.000 habitants i el 12 de febrer de 2020 el Consell de la Sindicatura de Comptes va aprovar l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament d'Elx, Exercici 2019. Posteriorment, el Consell de la Sindicatura va incloure en els programes anuals d'actuació de 2021 i 2022 fer un treball de seguiment de la situació dels controls bàsics de ciberseguretat d'aquest ajuntament i dels altres 14 analitzats.

La necessitat d'una ciberhigiene adequada

Addicionalment, la crisi provocada per l'epidèmia de COVID-19 i les mesures tecnològiques adoptades per les administracions públiques han posat de manifest amb absoluta claredat la total dependència de l'Administració respecte dels sistemes d'informació i comunicacions i el fort augment de la superfície d'exposició davant de les ciberamenaces. Per a fer front a aquesta realitat, les entitats públiques han d'implementar controls sobre la seguretat de la informació i les comunicacions d'acord amb les directrius establides en l'Esquema Nacional de Seguretat (ENS), tant per obligació legal com per raons d'autoprotecció i supervivència.

En aquests entorns actuals d'administració electrònica avançada prenen tot el sentit conceptes com la ciberresiliència i la ciberhigiene. Per ciberresiliència es pot entendre la capacitat d'una entitat per a evitar o resistir un ciberatac i recuperar-se'n en un temps

raonable per a continuar prestant els seus serveis. La ciberhigiene és un principi fonamental[1] relacionat amb la seguretat de la informació i equival a establir mesures rutinàries senzilles per a minimitzar els riscos de les ciberamenaces. De manera anàloga al que ocorre amb la higiene personal, les bones pràctiques de ciberhigiene poden impulsar una major immunitat en les entitats que les apliquen, la qual cosa redueix el risc davant d'un ciberatac.

Per tant, l'existència d'uns controls eficaços de ciberseguretat és un element essencial per a la prestació de serveis públics en una administració tecnològicament avançada. En aquest sentit, considerem que la implantació dels controls bàsics de ciberseguretat (CBCS) –en definitiva, un subconjunt de les mesures de seguretat obligatòries exigides per l'ENS– constitueix una mesura bàsica de ciberhigiene per a les administracions públiques.

2. RESPONSABILITATS DELS ÒRGANS SUPERIORS DE L'AJUNTAMENT EN RELACIÓ AMB ELS CONTROLS DE CIBERSEGURETAT

Els òrgans superiors de l'Ajuntament (en particular l'alcalde i la Junta de Govern) són els responsables que hi haja uns controls adequats sobre els sistemes d'informació i les comunicacions. D'acord amb les seues competències, han de garantir que el funcionament de l'entitat resulte conforme amb les normes aplicables i que els controls interns proporcionen una garantia raonable que la informació, els serveis i els sistemes d'informació que els donen suport complisquen les propietats següents, que coincideixen amb les cinc dimensions de la seguretat de la informació que estableix l'Esquema Nacional de Seguretat: confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat.

3. RESPONSABILITAT DE LA SINDICATURA DE COMPTES

D'acord amb el que es preveu en els programes anuals d'actuació de 2021 i 2022 hem realitzat el seguiment de la situació dels controls bàsics de ciberseguretat i de les recomanacions efectuades en l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament d'Elx. Exercici 2019.

La responsabilitat de la Sindicatura de Comptes és concloure sobre la situació dels controls bàsics de ciberseguretat revisats, proporcionant una avaluació sobre el seu disseny i eficàcia operativa, sobre el compliment de la normativa bàsica relativa a la seguretat de la informació i, si és el cas, formular recomanacions que contribuïsquen a esmenar les deficiències observades i a millorar els procediments de control.

Aquesta auditoria s'ha centrat en l'anàlisi de la situació actualitzada a 31 de desembre de 2021 dels huit CBCS revisats en l'auditoria de l'any 2019, relacionats amb les aplicacions i

[1] *Review of Cyber Hygiene Practices*, European Union Agency for Cybersecurity (ENISA), 2016.

sistemes que suporten el procés comptable-pressupostari, la gestió tributària i recaptadora i altres sistemes d'interés general.

Per a això, hem dut a terme el treball de conformitat amb els *Principis fonamentals de fiscalització de les institucions públiques de control extern* i amb les normes tècniques de fiscalització aprovades pel Consell de la Sindicatura recollides en el *Manual de fiscalització* de la Sindicatura de Comptes. Aquests principis exigeixen que complim els requeriments d'ètica, com també que planifiquem i executem l'auditoria amb la finalitat d'obtindre una seguretat limitada sobre la situació dels CBCS revisats.

Considerem que l'evidència d'auditoria obtinguda proporciona una base suficient i adequada per a fonamentar les nostres conclusions sobre l'estat dels controls bàsics de ciberseguretat, d'acord amb l'abast limitat que s'ha assenyalat.

Els procediments realitzats en una auditoria de seguretat limitada són reduïts en comparació amb els que es requereixen per a obtindre una seguretat raonable, però s'espera que el nivell de seguretat siga, d'acord amb el judici professional de l'auditor, significatiu per als destinataris de l'informe. La seguretat limitada no garanteix que una auditoria realitzada de conformitat amb els *Principis fonamentals de fiscalització dels òrgans de control extern* i amb les normes tècniques de fiscalització recollides en el *Manual de fiscalització* de la Sindicatura de Comptes detecte sempre un incompliment significatiu quan existisca.

En l'apèndix 1 es proporciona un major detall de la metodologia utilitzada. En l'apèndix 2 es detallen les constatacions de l'auditoria que sustenten les conclusions i les recomanacions d'aquest informe.

4. CONCLUSIONS

Encara que s'han realitzat progressos des de la nostra auditoria anterior i s'han atés parcialment algunes de les nostres recomanacions, l'índex de maduresa general dels controls bàsics de ciberseguretat és insuficient i ha de millorar per a aconseguir els nivells exigits per l'ENS

Com a resultat del treball realitzat, amb l'abast assenyalat en l'apartat anterior, cal concloure que l'**índex de maduresa general** en la gestió dels controls bàsics de ciberseguretat aconsegueix un **50,3%**, que es correspon amb un nivell de maduresa *N2, repetible però intuïtiu*; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment.

L'Ajuntament ha atés de manera parcial algunes de les nostres recomanacions i l'índex de maduresa general ha millorat des del 40,7% de la nostra auditoria de 2019, però l'índex de maduresa actual continua sent insuficient per a garantir un grau adequat de seguretat i aconseguir el 80% requerit per l'ENS. La comparació dels resultats detallats d'aquest treball amb els obtinguts l'any 2019 mostra una millora en quasi tots els controls, si bé la millora ha sigut insuficient i cap aconsegueix l'objectiu del 80%, atés el baix grau d'atenció

d'algunes de les nostres recomanacions (vegeu l'apartat 5 següent). Un dels controls, el CBCS 7, ha empitjorat lleugerament.

Els resultats detallats obtinguts per a cada un dels CBCS i la seua evolució es mostren en el quadre 1.

Quadre 1. Índex de maduresa dels controls bàsics de ciberseguretat

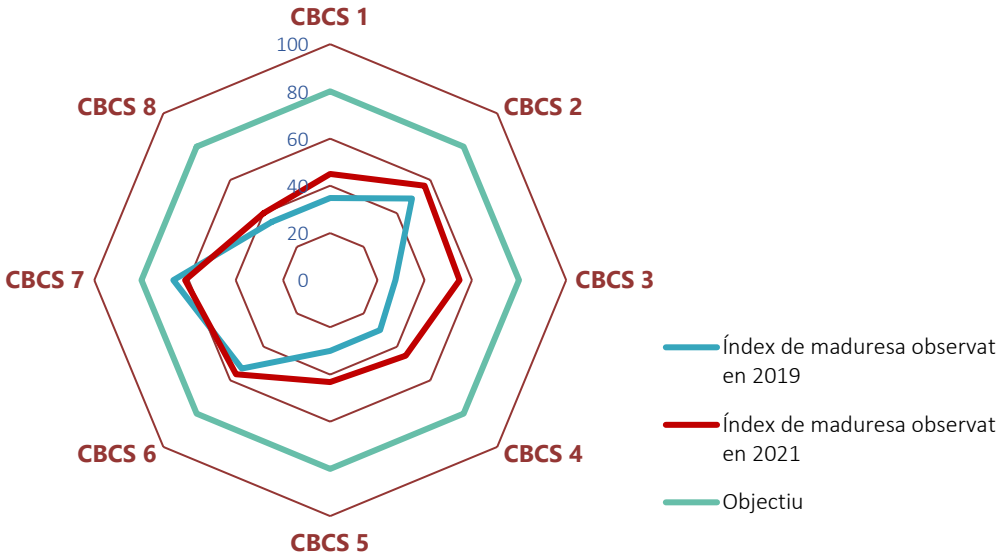
Control	2019 Índex de maduresa	2019 Nivell de maduresa	2019 Índex de compli-ment	2021 Índex de maduresa	2021 Nivell de maduresa	2021 Índex de compli-ment
CBCS 1 Inventari i control de dispositius físics	*34,8%*	***N1***	*43,4%*	45,0%	**N1**	56,3%
CBCS 2 Inventari i control de programari autoritzat i no autoritzat	*49,0%*	***N1***	*61,3%*	56,5%	**N2**	70,6%
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	*27,6%*	***N1***	*34,5%*	54,8%	**N2**	68,4%
CBCS 4 Ús controlat de privilegis administratius	*29,9%*	***N1***	*37,3%*	45,2%	**N1**	56,5%
CBCS 5 Configuracions segures del programari i maquinari	*30,0%*	***N1***	*37,5%*	43,2%	**N1**	54,0%
CBCS 6 Registre de l'activitat dels usuaris	*53,0%*	***N2***	*66,3%*	56,5%	**N2**	70,6%
CBCS 7 Còpies de seguretat de dades i sistemes	*66,5%*	***N2***	*83,1%*	61,5%	**N2**	76,9%
CBCS 8 Compliment normatiu i governança de ciberseguretat	*35,0%*	***N1***	*43,8%*	40,0%	**N1**	50,0%
General	40,7%	N1	50,9%	50,3%	N2	62,9%

L'índex de compliment dels CBCS és del 62,9%, que resulta de comparar l'índex de maduresa amb el nivell requerit o objectiu que té el sistema segons l'ENS, que és el 80%. Aquest índex ha millorat des del 50,9% del nostre informe anterior.

Han d'implantar-se millores amb major intensitat en aquells controls que presenten deficiències significatives i no aconsegueixen el nivell de maduresa N2 (CBCS 1, CBCS 4, CBCS 5 i CBCS 8). En l'apartat 5 es realitzen les recomanacions pertinents amb aquesta finalitat.

D'una manera gràfica, la situació observada dels controls, tant en aquesta auditoria com en la realitzada l'any 2019, queda reflectida en el gràfic 1.

Gràfic 1. Índex de maduresa dels controls bàsics de ciberseguretat



La nostra auditoria i els indicadors reflecteixen la situació a 31 de desembre de 2021.

L'Ajuntament d'Elx no té establida una governança adequada de la ciberseguretat, situació que s'ha d'esmenar. Els òrgans de govern han d'aprovar normes i procediments en relació amb la seguretat de la informació aplicables a tota l'organització per igual

Els òrgans superiors de l'Ajuntament (en particular l'alcalde i la Junta de Govern) són els responsables que hi haja uns controls adequats sobre els sistemes d'informació i les comunicacions, i la seua implicació, compromís i lideratge constitueixen, possiblement, el factor més important per a la implantació reeixida d'un sistema de gestió de la seguretat de la informació que garantisca la ciberresiliència de l'entitat.

El compromís i conscienciació amb la ciberseguretat també s'ha d'estendre a la direcció[2] (tal com es defineix en el glossari al final d'aquest informe), que són els responsables d'articular i facilitar l'execució de les activitats establides per l'alta direcció en matèria de ciberseguretat.

Encara que hem observat un cert compromís i conscienciació amb la ciberseguretat per part dels òrgans superiors de l'Ajuntament i en els tres departaments amb responsabilitats

[2] *Prontuario de ciberseguridad para entidades locales*, Centre Criptològic Nacional i Federació Espanyola de Municipis i Províncies, abril 2021.

en matèria de seguretat de la informació (informàtica, telecomunicacions i policia local), hi ha mancances rellevants com ara:

- Absència d'un marc normatiu i procedimental únic formalment aprovat. Encara que l'Ajuntament disposa de la política de seguretat de la informació aprovada per la Junta de Govern i té definits els rols en matèria de seguretat, no ha desenvolupat el marc normatiu (ús correcte d'equips, serveis, instal·lacions, usos indeguts, responsabilitats del personal) i procedimental (documents que detallen com es fan les tasques habituals, responsables, report de comportaments anòmals) requerit en l'ENS per a garantir una efectiva organització global de la seguretat de la informació.

  La falta de procediments que identifiquen les tasques habituals i els seus responsables fan que cada un dels tres departaments amb responsabilitats en matèria de seguretat de la informació seguisca criteris i procediments tècnics diferents. Aquesta situació repercuteix negativament en la valoració dels controls, atés que la ineficiència de controls en qualsevol de les àrees repercuteix en el risc i la valoració global del control.

- La necessitat que el comité de seguretat de la informació, òrgan imprescindible per a coordinar la seguretat de la informació en l'entitat, es reunisca regularment, a fi de conéixer l'estat de la seguretat de la informació de l'Ajuntament i prendre les decisions pertinents de manera oportuna. En una entitat de la grandària i complexitat de l'ajuntament hauria de reunir-se almenys mensualment.

  Tal com s'indica en la guia CCN-STIC 801, el comité coordina la seguretat de la informació de l'entitat i ha d'estar format, a més de pel responsable de seguretat de la informació, per representants de les tres àrees amb responsabilitats en matèria de seguretat de la informació, circumstància que actualment no es produeix.

- Les decisions en matèria de seguretat de la informació han de ser aplicades pels tècnics o les empreses adjudicatàries d'acord amb les directrius establides formalment per la corporació, pel comité o pel responsable de seguretat i no atenent els seus propis criteris.

És necessari, per tant, solucionar de manera urgent les mancances identificades, que tenen un impacte negatiu en el nivell de seguretat de la informació de l'Ajuntament, i atendre les recomanacions efectuades en aquest informe.

El grau de compliment de la normativa relativa a la seguretat de la informació és molt deficient

La revisió del compliment de legalitat en matèria relacionada amb la seguretat de la informació ha posat de manifest un nivell deficient de compliment de la normativa. Hi ha incompliments significatius generalitzats, que s'assenyalen en l'apartat 5, sobre els quals s'ha d'actuar per a esmenar-los ràpidament.

5. RECOMANACIONS I MESURES NECESSÀRIES PER AL COMPLIMENT DE LA LEGALITAT

Per a esmenar les deficiències de control identificades per la Sindicatura en aquesta auditoria i millorar els nivells de control assenyalats en l'apartat 4 anterior, reformulem les recomanacions que es van efectuar en l'auditoria de 2019, considerant les millores realitzades des de llavors. L'Ajuntament haurà de dedicar els esforços i recursos necessaris per a esmenar les deficiències pendents.

També s'assenyalen les mesures per al compliment de la legalitat que s'han d'adoptar.

Sobre l'inventari i control de dispositius físics (CBCS 1)

1. Aprovar formalment un procediment unificat per a la gestió de l'inventari i el control d'actius físics que reculla el procés actualment implantat i s'aplique a tots els sistemes d'informació de l'Ajuntament. També ha d'incloure els aspectes següents:

    - Incloure les revisions periòdiques del maquinari instal·lat, actualitzant degudament l'inventari i incloent-hi les dates d'aquestes revisions.

    - Estendre l'ús de l'eina automatitzada actualment disponible a l'Ajuntament de manera que incloga tots els sistemes de l'entitat, sense excepció.

    - Homogeneïtzar la gestió de l'inventari, amb independència que el procés siga realitzat per diferents departaments.

2. Finalitzar els treballs d'implantació de les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.

Sobre l'inventari i control de programari autoritzat (CBCS 2)

3. Elaborar i aprovar formalment un procediment per a la gestió integral del programari de l'entitat que establisca les mesures actualment implantades, s'aplique a totes les àrees per igual i incloga:

    - L'elaboració de llistes de programari autoritzat (llistes blanques), el procés d'autorització per a la instal·lació de programari, la implantació de les mesures tècniques que impedisquen l'execució del programari no autoritzat i la realització de revisions periòdiques.

    - La definició d'un pla de manteniment del programari que considere la totalitat de l'utilitzat a l'Ajuntament.

4. Finalitzar el procés de revisió i actualització de tots els sistemes que es troben fora del seu període de suport.

Sobre el procés continu d'identificació i solució de vulnerabilitats (CBCS 3)

5. Establir en un procediment formalment aprovat el procés actualment implantat per a la identificació i solució de vulnerabilitats. Aquest procés haurà d'aplicar-se de manera homogènia a la totalitat de sistemes de l'Ajuntament, definir els sistemes inclosos i considerar l'anàlisi prèvia a l'entrada en producció dels sistemes, el seguiment d'anuncis de fabricants i butlletins oficials en matèria de seguretat, la priorització basada en l'anàlisi de riscos, la resolució i la documentació de les vulnerabilitats tractades.

Sobre l'ús controlat de privilegis administratius (CBCS 4)

6. Elaborar i aprovar formalment un procediment que reculla les mesures actualment implantades, que s'aplique a tots els sistemes de l'entitat i que incloga:

   - L'eliminació de tots els usuaris no nominatius amb privilegis administratius de tots els sistemes. Totes les activitats de gestió hauran de realitzar-se amb usuaris nominatius.

   - Quan hi haja raons d'índole tècnica que impedisquen l'eliminació d'usuaris genèrics, el seu ús haurà d'estar controlat de manera que es mantinga el principi de traçabilitat de les accions en els sistemes.

   - La utilització, per a cada administrador de sistemes de l'entitat, de diferents comptes amb diferents nivells de seguretat depenent de les tasques a realitzar (gestió del domini i servidors, administració d'equips d'usuari o tasques ofimàtiques no administratives).

   - La política d'autenticació a aplicar a aquest tipus de comptes.

Sobre les configuracions segures del programari i maquinari (CBCS 5)

7. Aprovar i implantar un procediment de configuració segura o fortificació dels sistemes que considere la seguretat per defecte i el criteri de mínima funcionalitat. Per a això, es proposa el desenvolupament de guies d'instal·lació específiques per sistemes, basades en les recomanacions dels fabricants i en les recomanacions dels organismes de referència, com ara les guies STIC de les sèries 400, 500 i 600 del CCN.

   Paral·lelament, s'aconsella desenvolupar un procediment de gestió continuada de la configuració dels sistemes, particularment dels sistemes crítics. Aquest procediment ha de preveure la gestió de canvis en els sistemes i la revisió periòdica dels canvis realitzats, bé per mitjà d'un procediment manual o a través d'eines automatitzades de monitoratge de la configuració.

Sobre el registre de l'activitat dels usuaris (CBCS 6)

8. Aprovar formalment un procediment per al tractament de *logs* d'auditoria d'activitat dels usuaris, que especifique les accions actualment implantades, els sistemes afectats, la informació que es reté, el període de retenció, còpies de seguretat, gestió de drets d'accés al registre i implantació i documentació d'un procés de revisió dels *logs*. Per a la revisió de *logs* és aconsellable centralitzar-los en sistemes dedicats a aquest efecte.

Sobre la còpia de seguretat de dades i sistemes (CBCS 7)

9. Aprovar formalment un procediment per a la gestió de còpies de seguretat de dades i sistemes, aplicable a tota l'organització, que definisca, com a mínim, les dades i sistemes afectats, la periodicitat de les còpies, ubicacions, responsables, les proves de restauració a realitzar i els requisits de protecció de les còpies.

Sobre el compliment normatiu i governança de la ciberseguretat (CBCS 8)

10. Implantar les mesures necessàries per a donar compliment als requisits del Reial Decret 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat. Específicament, l'Ajuntament ha de:

    - Elaborar una declaració d'aplicabilitat i adoptar les mesures de seguretat que s'hi descriguen.

    - Realitzar les auditories de compliment previstes en l'article 34 del Reial Decret 3/2010.

    - Publicar en la seu electrònica la certificació de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS de 13 d'octubre de 2016.

11. En relació amb la protecció de dades personals, l'Ajuntament ha d'adaptar-se al que s'estableix en l'RGPD i la Llei Orgànica 3/2018, de 5 de desembre. En particular:

    - Aprovar el registre d'activitats de tractament amb la informació requerida per l'RGPD i publicar aquest registre, d'acord amb l'article 31.2 de la Llei Orgànica 3/2018.

    - Realitzar una anàlisi de riscos sobre els seus tractaments de dades personals i, si és el cas, les avaluacions d'impacte dels tractaments, d'acord amb els articles 32.2 i 35 de l'RGPD.

    - Aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD.

    - Planificar i executar auditories de compliment en matèria de protecció de dades.

12. Dur a terme les auditories del registre de factures exigides per la Llei 25/2013, de 27 de desembre.

Priorització de les recomanacions

A fi que puguen establir-se accions basades en criteris de cost/benefici, en el gràfic 2 es mostra la classificació de les recomanacions segons els criteris combinats de **risc potencial que cal mitigar** i **cost estimat de la implantació**. Aquest gràfic s'ha actualitzat respecte al treball realitzat l'any 2019, adaptant la relació risc/cost de cada recomanació i considerant les millores realitzades des de la revisió anterior. No s'hi inclouen els punts 10, 11 i 12 anteriors, ja que són mesures de compliment obligat.

Gràfic 2. Riscos que s'atenen i cost d'implantació de les recomanacions

Seguiment de recomanacions anteriors

Hem realitzat un seguiment de les recomanacions efectuades en l'informe d'auditoria de l'any 2019.

Tal com es mostra en el quadre 2, de les dotze recomanacions realitzades en aquell informe, sis no s'han atés i en sis s'han realitzat accions parcials de millora; no hi ha cap recomanació atesa completament.

Actuacions en curs

Encara que no s'han tingut en compte en el càlcul dels indicadors que es mostren en l'apartat 4, hem verificat que en el moment de finalització del treball de camp de l'auditoria s'han iniciat o planificat actuacions en matèria de ciberseguretat en diversos àmbits que

atendrien algunes de les recomanacions anteriors. Aquestes actuacions es troben alineades amb els objectius de l'Ajuntament per a l'adequació a l'ENS i algunes s'han iniciat a conseqüència de les recomanacions realitzades en l'auditoria de l'any 2019. La implantació efectiva d'aquestes actuacions tindrà un impacte positiu en el nivell de ciberseguretat de l'entitat.

Enumerem a continuació les que es troben en execució i que per la seua rellevància han de ser destacades en l'Informe:

- Contractació de serveis entre els quals s'inclou el manteniment de la infraestructura actual, la renovació de la seguretat dels centres de dades i la millora del cablejat entre dos centres de dades de l'entitat, la qual cosa possibilitaria la integració de les tres àrees en una mateixa xarxa.

- Millora dels usuaris amb perfils d'administració. El departament d'informàtica ha iniciat proves per a establir diferents nivells de permisos en els seus propis usuaris, en funció de la tasca que hagen de realitzar, evitant validar-se en el sistema amb perfils d'administració per a tasques bàsiques que no requerisquen aquests privilegis.

- El departament d'informàtica ha integrat un SIEM en els seus sistemes, si bé ha de definir una política de *logs* d'auditoria i configurar-lo per a aprofitar la informació que proporciona.

- El departament d'informàtica ha activat el control d'aplicacions en els sistemes de la seua competència, si bé el control és limitat i s'ha de completar amb una política de gestió de programari que indique les aplicacions permeses i bloquejades per l'organització.

- Implantació d'un sistema NAC (*network access control*). El servei de telecomunicacions ha iniciat el procés d'actualització de tota l'electrònica de xarxa de l'entitat. Aquest canvi implica, a més de l'actualització de tots els *switches*, la integració d'aquests en una consola de gestió centralitzada. Els dispositius s'han configurat de manera que impedeixen la connexió a la xarxa de qualsevol dispositiu no autoritzat.

- Millora en les còpies de seguretat: el departament d'informàtica ha migrat en 2022 el programari de còpies de seguretat dels sistemes de la seua competència. No obstant això, aquesta millora únicament afecta els seus propis sistemes i, tal com s'ha recomanat, la corporació ha d'aprovar un procediment aplicable a tots els departaments i que establisca les directrius sobre aquest tema.

- L'Ajuntament està en fase d'actualització de determinats sistemes operatius fora de suport.

- L'Ajuntament ha desplegat el servei del CCN-Cert microCLAUDIA, per a la protecció contra codi nociu de tipus *ransomware*, en tots els equips de l'organització.

Quadre 2. Seguiment de recomanacions

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'Informe
1	Aprovar formalment un procediment unificat per a la gestió de l'inventari i el control d'actius físics que reculla el procés complet i s'aplique a tots els sistemes d'informació de l'Ajuntament. A l'hora d'establir aquest procés és necessari considerar els aspectes següents: • Incloure les revisions periòdiques del maquinari instal·lat, actualitzant degudament l'inventari i incloent-hi les dates d'aquestes revisions. • Fer extensiu l'ús de l'eina automatitzada de manera que incloga tots els sistemes de l'entitat. • Homogeneïtzar la gestió de l'inventari, amb independència que el procés el realitzen diferents departaments.	Encara que hi ha cert control sobre els actius físics de la xarxa corporativa en els diferents departaments, no s'ha elaborat un procediment que reculla el procés actual implantat i que s'aplique de manera homogènia a totes les àrees de l'entitat.	**No aplicada**	Es manté la redacció feta en 2019.
2	Implantar les solucions que permeten restringir l'accés de dispositius físics no autoritzats a la xarxa corporativa.	El departament de telecomunicacions ha iniciat la integració d'un NAC en la xarxa i el departament d'informàtica es troba en fase de proves d'un sistema de control de dispositius. No obstant això, aquests treballs no han finalitzat o no es troben implantats en tota l'entitat. Les mesures per a impedir connexions de dispositius no autoritzats a la xarxa corporativa no s'han establit en un procediment formalment aprovat per la corporació.	**Aplicada parcialment**	S'actualitza la redacció feta en 2019.
3	Elaborar i aprovar un procediment per a la gestió integral del programari de l'entitat que incloga: • L'elaboració de llistes de programari autoritzat (llistes blanques), el procés d'autorització per a la instal·lació de programari, la implantació de les mesures tècniques que impedisquen l'execució del programari no autoritzat i la realització de revisions periòdiques. • La definició d'un pla de manteniment del programari que considere la totalitat de l'utilitzat, incloent-hi tant el gestionat per mitjà de	L'Ajuntament ha realitzat accions que milloren, encara que de manera limitada, el control sobre les aplicacions instal·lades en tots els dispositius de l'entitat. No obstant això, les mesures no s'apliquen a tots els departaments per igual, ni existeix un procediment aprovat que establisca aquestes mesures.	**Aplicada parcialment**	S'actualitza la redacció feta en 2019.

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'Informe
	licitacions i clàusules contractuals com la resta de programari utilitzat a l'Ajuntament.			
4	Revisar i actualitzar tots els sistemes que es troben fora del seu període de suport.	Encara que s'ha actualitzat gran part dels sistemes que estaven fora de suport durant l'auditoria anterior, encara es mantenen en producció sistemes que han de ser actualitzats.	**Aplicada parcialment**	S'actualitza la redacció feta en 2019.
5	Establir un procediment d'identificació i solució de vulnerabilitats que s'aplique de manera integral a la totalitat de sistemes de l'Ajuntament i que considere, com a mínim, els aspectes següents: • La identificació de vulnerabilitats, incloent-hi l'escaneig per mitjà d'eines específiques, anàlisi prèvia a l'entrada en producció dels sistemes i el seguiment d'anuncis dels fabricants i butlletins oficials en matèria de seguretat. • La priorització de les vulnerabilitats identificades basada en l'anàlisi de risc, així com la resolució i documentació, identificant dates, prioritat, responsable, solució, etc. • L'ús d'eines que permeten la gestió unificada i automatitzada de pedaços de seguretat, de manera que s'apliquen a tots els sistemes de l'entitat, encara que aquests els gestionen diferents departaments.	L'Ajuntament ha implantat una eina que introdueix millores en el procés d'identificació i solució de vulnerabilitats, pedaços i actualitzacions. A més, aquesta eina afecta la totalitat de sistemes de l'entitat. No obstant això, no s'ha aprovat un procediment de gestió de vulnerabilitats que incloga les recomanacions proposades en la nostra auditoria.	**Aplicada parcialment**	S'actualitza la redacció feta en 2019.
6	Formalitzar un procediment unificat de gestió d'usuaris amb privilegis d'administració que establisca les directrius per a tots els sistemes de l'entitat i que incloga: • L'eliminació, sempre que siga possible des del punt de vista tècnic, de tots els usuaris no nominatius amb privilegis administratius de tots els sistemes. Totes les activitats de gestió s'han de realitzar amb usuaris nominatius. • Quan hi haja raons d'índole tècnica que impedisquen l'eliminació d'usuaris genèrics, el seu ús ha d'estar controlat de manera que es mantinga el principi de traçabilitat de les accions en els sistemes.	L'Ajuntament no ha aprovat un procediment que definisca la gestió d'usuaris amb privilegis administratius ni es revisen periòdicament els usuaris amb aquests privilegis. No obstant això, ha realitzat algunes accions encaminades a millorar aquest control.	**Aplicada parcialment**	S'actualitza la redacció feta en 2019.

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'Informe
	• La utilització, per a cada administrador de sistemes de l'entitat, de diferents comptes amb diferents nivells de seguretat depenent de les tasques a realitzar (gestió del domini i servidors, administració d'equips d'usuari o tasques ofimàtiques no administratives). • La política d'autenticació a aplicar a aquest tipus de comptes.			
7	Aprovar i implantar un procediment de configuració segura o fortificació dels sistemes que considere la seguretat per defecte i el criteri de mínima funcionalitat. Per a això, es proposa el desenvolupament de guies d'instal·lació específiques per sistemes, basades en les recomanacions dels fabricants i en les recomanacions dels organismes de referència, com ara les guies STIC de les sèries 400, 500 i 600 del CCN. Paral·lelament, s'aconsella desenvolupar un procediment de gestió continuada de la configuració dels sistemes, particularment dels sistemes crítics de l'entitat. Aquest procediment ha de preveure la gestió de canvis en els sistemes i la revisió periòdica dels canvis realitzats, bé per mitjà d'un procediment manual o a través d'eines automatitzades de monitoratge de la configuració.	Sense variació	**No aplicada**	Es manté la redacció feta en 2019.
8	Aprovar formalment un procediment per al tractament de *logs* d'auditoria d'activitat dels usuaris, que especifique, com a mínim, els sistemes afectats, la informació que es reté, el període de retenció, còpies de seguretat, gestió de drets d'accés al registre i implantació i documentació d'un procés de revisió dels *logs*. Per a la revisió de *logs* és aconsellable centralitzar-los en sistemes dedicats a aquest efecte.	L'Ajuntament ha implantat una eina SIEM per a la gestió de *logs* d'auditoria. No obstant això, no s'inclouen tots els sistemes crítics ni el seu ús s'ha formalitzat en un procediment aprovat que indique quins sistemes s'hi inclouen, responsables, mesures de protecció, etc.	**Aplicada parcialment**	S'actualitza la redacció feta en 2019.
9	Aprovar formalment un procediment per a la gestió de còpies de seguretat de dades i sistemes, que definisca, com a mínim, les dades i sistemes afectats, la periodicitat de les còpies, ubicacions, responsables, les proves de restauració a realitzar i els requisits de protecció de les còpies.	Cada departament realitza les còpies de seguretat de les seues dades atenent els seus propis criteris. En el departament de policia el procés és manual, no gestionable, i la seua eficàcia depén de la bona voluntat de les persones que el gestionen. Segueix sense existir un procediment aprovat per la	**No aplicada**	S'actualitza la redacció feta en 2019 per a recollir la necessitat d'un procediment aplicable a tots els departaments.

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'Informe
		corporació per a la gestió de còpies de seguretat que s'aplique a totes les àrees de l'Ajuntament per igual i definisca els criteris necessaris (dades, responsables, periodicitat, mesures de protecció, etc.).		
10	Implantar les mesures necessàries per a donar compliment als requisits de l'RD 3/2010, de 8 de gener, que regula l'Esquema Nacional de Seguretat. Específicament, l'Ajuntament ha de: • Elaborar una declaració d'aplicabilitat i adoptar les mesures de seguretat que s'hi descriuen. • Realitzar les auditories de compliment previstes en l'article 34 de l'RD 3/2010. • Publicar en la seu electrònica les declaracions de conformitat i els distintius corresponents, d'acord amb la Instrucció Tècnica de Seguretat de conformitat amb l'ENS del 13 d'octubre de 2016.	Sense variació	**No aplicada**	Es manté la redacció feta en 2019.
11	En relació amb la protecció de dades personals, l'Ajuntament ha d'adaptar-se al que s'estableix en l'RGPD i la LO 3/2018, de 5 de desembre. En particular ha de: • Aplicar el registre d'activitats de tractament amb la informació requerida per l'RGPD i publicar aquest registre, d'acord amb l'article 31.2 de la LO 3/2018. • Realitzar una anàlisi de riscos sobre els seus tractaments de dades personals i, si és el cas, les avaluacions d'impacte dels tractaments, d'acord amb els articles 32.2 i 35 de l'RGPD. • Aplicar les mesures organitzatives i tècniques necessàries per a protegir les dades personals, d'acord amb l'article 24.1 de l'RGPD. • Planificar i executar auditories de compliment en matèria de protecció de dades.	Sense variació	**No aplicada**	Es manté la redacció feta en 2019.

	Recomanacions de l'informe anterior	Situació a 31 de desembre de 2021 respecte a l'informe anterior	Estat de la recomanació	Conseqüència en l'Informe
14	Dur a terme les auditories del registre de factures exigides per la Llei 25/2013, de 27 de desembre.	Sense variació	**No aplicada**	Es manté la redacció feta en 2019.

APÈNDIX 1
Metodologia aplicada

Introducció

Cada vegada un major nombre d'aspectes de la gestió pública es realitza amb el suport de complexos sistemes informatitzats, i la connectivitat per internet s'ha convertit en una característica fonamental d'aquests sistemes d'informació. Aquesta circumstància ha comportat un gran creixement de tot tipus d'amenaces provinents del ciberespai, majors riscos de ciberseguretat i s'han multiplicat els incidents de seguretat de què són víctimes els sistemes d'informació i comunicacions de les entitats públiques, amb greus repercussions potencials –i en molts casos, reals– tant econòmiques com en la prestació dels serveis públics.

Les entitats locals, i els ajuntaments en particular, no són alienes a aquesta problemàtica de la ciberseguretat en la seua mateixa operatòria, per la qual cosa han d'implementar controls sobre la seguretat de la informació i les comunicacions d'acord amb les directrius establides en l'Esquema Nacional de Seguretat, que és **de compliment obligat**.

Per aquestes raons, és imperatiu que els responsables dels ajuntaments gestionen els riscos associats amb el funcionament i ús dels sistemes d'informació que s'utilitzen per a desenvolupar i prestar els serveis públics. Així mateix, han d'establir controls de ciberseguretat adequats per a mantindre els sistemes d'informació protegits davant de les amenaces de seguretat i evitar la interrupció en els serveis prestats als ciutadans i ajuntaments.

La gestió dels riscos de ciberseguretat comprén una àmplia gamma d'activitats orientades a protegir els sistemes d'informació i les dades davant d'accessos no autoritzats i altres amenaces cibernètiques, detectar anomalies i incidents que els afecten negativament i mitigar-ne l'impacte, i també respondre i recuperar-se d'incidents.

Tot i que l'adopció de mesures de seguretat adequades fa més resilients les organitzacions davant dels ciberatacs, l'anàlisi dels incidents produïts que es realitza en els informes INES[3] del CCN revela que les organitzacions no sempre implementen ni tan sols les mesures més bàsiques que podrien haver evitat o mitigat el mal causat. D'altra banda, el fet que els ciberatacs es mantinguen en molts casos sense ser detectats durant molt de temps pot ser evidència que les mesures bàsiques no estan implementades correctament.

En definitiva, l'existència d'uns controls eficaços de ciberseguretat és un element essencial per a la prestació de serveis públics d'una administració tecnològicament avançada. En aquest sentit considerem que **la implantació dels controls bàsics de ciberseguretat (CBCS)** –un subconjunt de les mesures de seguretat obligatòries exigides per l'ENS– **constitueix una mesura bàsica de ciberhigiene** per a les administracions públiques.

[3] Informe Nacional de l'Estat de Seguretat dels Sistemes de les TIC del CCN.

Objectiu de l'auditoria

D'acord amb el que es preveu en els programes anuals d'actuació de 2021 i 2022, el nostre objectiu ha sigut realitzar el seguiment de la situació dels controls bàsics de ciberseguretat i de les recomanacions efectuades en l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament d'Elx. Exercici 2019, així com obtindre una seguretat limitada i concloure sobre la situació dels controls bàsics de ciberseguretat revisats. Per a això n'hem avaluat tant el disseny[4] com l'eficàcia operativa[5] per a garantir la integritat, disponibilitat, autenticitat, confidencialitat i traçabilitat de la informació, els serveis i els sistemes d'informació que els donen suport. També hem revisat el compliment de la normativa bàsica relativa a la seguretat de la informació.

Així mateix, hem formulat recomanacions que contribuïsquen a esmenar les deficiències observades i a millorar els procediments de control, tenint en consideració les millores introduïdes des de la nostra auditoria anterior.

Aquesta auditoria s'ha centrat en l'anàlisi de la situació actualitzada dels huit CBCS revisats en l'auditoria de l'any 2019, relacionats amb les aplicacions i sistemes que suporten el procés comptable-pressupostari, la gestió tributària i recaptadora i altres sistemes d'interés general.

Abast

L'auditoria s'ha centrat en l'anàlisi de la situació dels huit CBCS:

CBCS 1	Inventari i control de dispositius físics
CBCS 2	Inventari i control de programari autoritzat i no autoritzat
CBCS 3	Procés continu d'identificació i solució de vulnerabilitats
CBCS 4	Ús controlat de privilegis administratius
CBCS 5	Configuracions segures del programari i maquinari
CBCS 6	Registre de l'activitat dels usuaris
CBCS 7	Còpies de seguretat de dades i sistemes
CBCS 8	Compliment normatiu i governança de ciberseguretat

Atesa la naturalesa de l'objecte material que cal revisar –la gran amplitud, complexitat i diversitat dels sistemes d'informació d'un ens local de grans dimensions– ha sigut necessari delimitar i concretar quins sistemes s'havien d'analitzar. En aquest sentit, hem analitzat les aplicacions que suporten els processos de gestió comptable i pressupostària i la gestió tributària i recaptadora, així com els controls que tenen implantats.

[4] L'avaluació del disseny d'un control implica la consideració per l'auditor de si el control, de manera individual o en combinació amb altres controls, és capaç de previndre de manera eficaç, o de detectar i corregir, la materialització dels riscos previstos. És a dir, és capaç de complir l'objectiu de control.

[5] L'auditor comprova que el control existeix i que l'entitat l'està utilitzant.

Addicionalment, per la seua importància per al bon funcionament dels sistemes d'informació i la ciberseguretat, hem analitzat els tipus d'elements següents:

- controlador de domini
- programari de virtualització
- equips d'usuari (una mostra)
- elements de la xarxa de comunicacions (una mostra)
- elements de seguretat (una mostra)

L'abast específic d'aquest treball de seguiment de recomanacions ha estat condicionat per l'organització funcional de l'Ajuntament. D'acord amb aquesta organització, la gestió de la seguretat de la informació comprén tres àrees: informàtica, telecomunicacions i policia local.

Cada una de les àrees anteriors realitza la gestió dels seus propis sistemes, sense seguir criteris formalment aprovats per la corporació o impulsats pel comité de seguretat. Hi ha, per tant, diferents responsabilitats i aquestes recauen en diferents tècnics que apliquen els procediments atenent els seus propis criteris.

La situació anterior és particularment deficient, no per l'organització en si de les àrees de l'Ajuntament, aspecte que no s'ha avaluat en aquest informe, sinó perquè la inexistència de polítiques que s'apliquen de manera uniforme a totes les àrees de l'Ajuntament implica que una debilitat en un control en qualsevol de les àrees afecta tot el sistema d'informació.

Àmbit temporal

Quant a l'àmbit temporal del treball, les conclusions es refereixen a la situació dels controls a 31 de desembre de 2021, data sobre la qual s'han calculat els indicadors de l'Informe, ja que fins a aquell moment s'ha admés qualsevol evidència disponible. Per tant, amb caràcter general l'Informe reflecteix la situació en aquell moment, ja que és freqüent que, des que s'inicia el treball de camp, determinades deficiències observades i assenyalades als gestors siguen esmenades i són considerades d'aquesta manera en les conclusions i en els indicadors.

Addicionalment, les constatacions de l'auditoria, les conclusions i l'esborrany previ de l'informe es discuteixen amb els responsables de l'entitat auditada, d'acord amb el que s'estableix en el nostre *Manual de fiscalització*.

Metodologia

Hem dut a terme el treball de conformitat amb els *Principis fonamentals de fiscalització de les institucions públiques de control extern* i amb les normes tècniques de fiscalització aprovades pel Consell de la Sindicatura i recollides en el *Manual de fiscalització* de la Sindicatura de Comptes. Aquests principis exigeixen que complim els requeriments d'ètica,

com també que planifiquem i executem l'auditoria amb la finalitat d'obtindre una seguretat limitada sobre la situació dels CBCS revisats.

Som independents de l'entitat auditada, de conformitat amb els requeriments d'ètica i protecció de la independència exigits per la normativa reguladora de l'activitat d'auditoria dels òrgans de control extern i per l'article 8 de l'LSC.

La Unitat d'Auditoria de Sistemes d'Informació de la Sindicatura de Comptes (UASI) ha realitzat aquesta auditoria dels controls bàsics de ciberseguretat seguint la metodologia establida en la guia pràctica de fiscalització GPF-OCEX 5313, "Revisió dels controls bàsics de ciberseguretat (CBCS)".

Hem avaluat la situació dels CBCS utilitzant el model de nivell de maduresa dels processos, definit en l'apèndix 1 de la guia esmentada, ja que, a més de ser un sistema àmpliament acceptat, permet establir objectius, realitzar comparacions entre entitats diferents i veure'n l'evolució al llarg del temps.

La guia pràctica de fiscalització dels OCEX 5313

La guia pràctica de fiscalització dels OCEX GPF-OCEX 5313, "Revisió dels controls bàsics de ciberseguretat", va ser aprovada per la Conferència de Presidents dels Òrgans de Control Extern el 12 de novembre de 2018, i forma part del *Manual de fiscalització* de la Sindicatura de Comptes, que es pot consultar en el nostre web. Per a major detall sobre la metodologia utilitzada ens remetem a aquesta guia.

El contingut de la GPF-OCEX 5313, fonamentalment relacionat amb l'auditoria de la seguretat dels sistemes d'informació, és coherent amb els postulats de l'ENS. No obstant això, atesa l'amplitud de l'ENS, que està format per 75 mesures de seguretat, per a la seua inclusió en els CBCS es va seleccionar una sèrie limitada de controls. Per a triar els més rellevants es va atendre el marc conceptual establit per la prestigiosa organització Center for Internet Security (CIS),[6] que defineix, prioritza i classifica vint controls de ciberseguretat segons la seua importància per a fer front a les ciberamenaces. L'avantatge principal és que estan orientats a mitigar els atacs més comuns i nocius amb la intenció d'automatitzar-los al màxim possible. Segons el CIS, amb caràcter general, les organitzacions que apliquen només els cinc primers controls poden reduir el seu risc davant ciberatacs al voltant del 85%. Si s'implementen els vint controls el risc es pot reduir un 94%.

Es van triar els set CBCS més rellevants i se'n va afegir un huité relacionat amb el compliment normatiu, per la seua importància en una administració pública. En aquest informe hem destacat, a més, els aspectes relacionats amb la governança de ciberseguretat establits en l'ENS i en l'RGPD.

[6] Center for Internet Security.

Alineació dels CBCS amb l'Esquema Nacional de Seguretat

Atés que l'ENS és de compliment obligat per a tots els ens públics, s'ha tingut especial cura que la metodologia d'auditoria dels controls bàsics de ciberseguretat estiguera plenament alineada amb l'ENS. Aquesta alineació facilita la realització de les auditories de ciberseguretat per part de la Sindicatura i coadjuva a la implantació de l'ENS en els ens auditats, ja que pràcticament tots els subcontrols o controls detallats que verifica la Sindicatura els requereix l'ENS. D'aquesta manera, els huit controls bàsics de ciberseguretat presenten una correspondència (no exacta) amb les referències següents de l'ENS:

Quadre 3. Els CBCS i l'ENS

Control		Mesura de seguretat de l'ENS*
CBCS 1	Inventari i control de dispositius físics	op.exp.1
CBCS 2	Inventari i control de programari autoritzat i no autoritzat	op.exp.1 op.exp.2
CBCS 3	Procés continu d'identificació i solució de vulnerabilitats	mp.sw.2 op.exp.4
CBCS 4	Ús controlat de privilegis administratius	op.acc.4 op.acc.5
CBCS 5	Configuracions segures del programari i maquinari	op.exp.2 op.exp.3
CBCS 6	Registre de l'activitat dels usuaris	op.exp.8 op.exp.10
CBCS 7	Còpies de seguretat de dades i sistemes	mp.info.9
CBCS 8	Compliment normatiu i governança de la ciberseguretat	

* Aquestes sigles identifiquen cada una de les mesures de seguretat de l'annex I de l'ENS.

Els CBCS com a mesures de ciberhigiene

L'European Union Agency for Cybersecurity (ENISA) assenyala[7] que "la ciberhigiene és un principi fonamental relatiu a la seguretat de la informació i, com a analogia amb la higiene personal, és l'equivalent a establir simples mesures rutinàries per a minimitzar els riscos de les ciberamenaces. La suposició subjacent és que les bones pràctiques de ciberhigiene poden proporcionar immunitat en les entitats que les apliquen" i reduir els ciberriscos.[8]

[7] *Review of Cyber Hygiene Practices*, ENISA, desembre de 2016. Vegeu la pàgina 14.

[8] Segons experts citats en l'informe DOD Needs to Take Decisive Actions to Improve Cyber Hygiene de la US Government Accountability Office (2020), fins al 90% dels ciberatacs podrien evitar-se implantant mesures de ciberhigiene adequades.

Sintetitzant, la ciberhigiene es refereix al conjunt de pràctiques i accions bàsiques que una organització ha d'implantar per a fer front als riscos de ciberseguretat més comuns i generalitzats a què s'enfronta hui dia.[9]

En aquesta direcció, ENISA estableix deu punts d'acció per a una ciberhigiene adequada. Com s'observa en el quadre 4, dels set CBCS, sense comptar el de compliment normatiu, cinc són coincidents amb els punts d'acció prioritaris recomanats per ENISA com a bones pràctiques de ciberhigiene.

Quadre 4. Punts d'acció d'ENISA

ENISA	CBCS
1. Tindre un registre de tot el maquinari	CBCS 1
2. Tindre un registre de tot el programari per a assegurar-se que s'hi han posat correctament els pedaços	CBCS 2
3. Utilitzar guies de configuració segura i fortificació per a tots els dispositius	CBCS 5
4. Gestionar les dades que entren i ixen de la xarxa	–
5. Escanejar tots els correus electrònics entrants	–
6. Minimitzar els usuaris administradors	CBCS 4
7. Realitzar còpies de seguretat de dades regularment i fer proves de restauració	CBCS 7

A l'efecte d'aquest treball, considerem que els CBCS constitueixen un conjunt de pràctiques i accions bàsiques per a mantindre una ciberhigiene adequada.

També pot consultar-se el nostre Informe d'auditoria dels controls bàsics de ciberseguretat dels majors ajuntaments de la Comunitat Valenciana. Exercicis 2019 i 2020, en l'apartat 5 del qual expliquem per què són importants els CBCS.

Criteris d'auditoria: els controls bàsics de ciberseguretat i els seus subcontrols

Utilitzem els controls bàsics de ciberseguretat com a criteris d'auditoria o criteris d'avaluació. Els CBCS són controls globals formats per 26 subcontrols detallats, tal com es mostra en el quadre següent. Totes les nostres comprovacions tenen com a objectiu contrastar la situació real dels subcontrols en l'entitat davant de les bones pràctiques recollides en la GPF-OCEX 5313, en què s'especifica amb el màxim detall els aspectes comprovats en cada control.

[9] Carnegie Mellon University Software Engineering Institute, *Cyber Hygiene: A Baseline Set of Practices*, 2017.

Quadre 5. Els CBCS i els seus subcontrols

Control	Objectiu del control	Subcontrol	
CBCS 1 Inventari i control de dispositius físics	Gestionar activament tots els dispositius de maquinari en la xarxa, de manera que només els dispositius autoritzats tinguen accés a la xarxa.	CBCS 1-1: Inventari d'actius físics autoritzats	L'entitat disposa d'un inventari d'actius físics autoritzats complet, actualitzat i detallat.
		CBCS 1-2: Control d'actius físics no autoritzats	L'entitat disposa de mesures de seguretat per a controlar (detectar i restringir) l'accés de dispositius físics no autoritzats.
CBCS 2 Inventari i control de programari autoritzat	Gestionar activament tot el programari en els sistemes, de manera que només es puga instal·lar i executar programari autoritzat.	CBCS 2-1: Inventari de programari autoritzat	L'entitat disposa d'un inventari de programari complet, actualitzat i detallat.
		CBCS 2-2: Programari suportat pel fabricant	El programari utilitzat per l'entitat té suport del fabricant. En cas contrari, es marca en l'inventari com fora de suport.
		CBCS 2-3: Control de programari no autoritzat	L'entitat disposa de mecanismes que impedeixen la instal·lació i execució de programari no autoritzat.
CBCS 3 Procés continu d'identificació i solució de vulnerabilitats	Disposar d'un procés continu per a obtindre informació sobre noves vulnerabilitats, identificar-les, remeiar-les i reduir la finestra d'oportunitat als atacants.	CBCS 3-1: Identificació de vulnerabilitats	Existeix un procés per a identificar les vulnerabilitats dels components del sistema que assegura que aquestes són identificades en temps oportú.
		CBCS 3-2: Priorització	Les vulnerabilitats identificades són analitzades i prioritzades per a la resolució atenent el risc que suposen per a la seguretat del sistema.
		CBCS 3-3: Resolució de vulnerabilitats	Es realitza un seguiment de la correcció de les vulnerabilitats identificades, de manera que es garanteix que es resolen en el temps previst en el procediment.
		CBCS 3-4: Pedaços	L'entitat disposa de procediments i eines que permeten aplicar els pedaços de seguretat publicats pels fabricants en un temps raonable.
CBCS 4 Ús controlat de privilegis administratius	Desenvolupar processos i utilitzar eines per a identificar, controlar, previndre i corregir l'ús i configuració de privilegis administratius en ordinadors, xarxes i aplicacions.	CBCS 4-1: Inventari i control de comptes d'administració	Els privilegis d'administració estan limitats adequadament i l'entitat disposa d'un inventari de comptes d'administració que facilita el correcte control.
		CBCS 4-2: Canvi de contrasenyes per defecte	Les contrasenyes per defecte dels comptes que no s'utilitzen o són estàndard es canvien abans de l'entrada en producció del sistema.
		CBCS 4-3: Ús dedicat de comptes d'administració	Els comptes d'administració només es realitzen per a les tasques que són estrictament necessàries.
		CBCS 4-4: Mecanismes d'autenticació	Els comptes d'administració estan subjectes a mecanismes d'autenticació robustos, que impedeixen l'accés no autoritzat per mitjà d'aquests comptes.
		CBCS 4-5: Auditoria i control	L'ús dels comptes d'administració està subjecte a auditoria i control de les activitats realitzades.

Control	Objectiu del control	Subcontrol	
CBCS 5 Configuracions segures del programari i maquinari de dispositius mòbils, portàtils, equips de taula i servidors	Establir, implantar i gestionar la configuració de seguretat, per mitjà d'un procés de control de canvis i gestió de la configuració rigorós, amb l'objectiu de previndre atacs a través de l'explotació de serveis i configuracions vulnerables.	CBCS 5-1: Configuració segura	L'entitat ha definit, documentat i implantat estàndards de configuració segura per a tots els sistemes operatius i programari.
		CBCS 5-2: Gestió de la configuració	L'entitat disposa de mecanismes que li permeten detectar canvis no autoritzats o erronis de la configuració i la seua correcció (retorn a la configuració segura) en un període de temps oportú.
CBCS 6 Registre de l'activitat dels usuaris (manteniment, monitoratge i anàlisi dels *logs* d'auditoria)	Recollir, gestionar i analitzar *logs* d'esdeveniments que poden ajudar a detectar, entendre o recuperar-se d'un atac.	CBCS 6-1: Activació de *logs* d'auditoria	El *log* d'auditoria està activat en tots els sistemes i dispositius de xarxa i conté el detall suficient per a la detecció, anàlisi, investigació i prevenció de ciberatacs.
		CBCS 6-2: Emmagatzematge de *logs*: retenció i protecció	Els *logs* es conserven durant el temps indicat en la política de retenció, de manera que es troben disponibles per a la consulta i anàlisi. Durant aquest període, el control d'accés garanteix que no es produeixen accessos no autoritzats.
		CBCS 6-3: Centralització i revisió de *logs*	Els *logs* de tots els sistemes són revisats periòdicament per a detectar anomalies i possibles riscos de seguretat del sistema. Es disposa de mecanismes per a la centralització dels *logs* d'auditoria, de manera que se'n facilite la revisió.
		CBCS 6-4: Monitoratge i correlació	L'entitat disposa d'un SIEM (*security information and event management*) o una eina d'analítica de *logs* per a realitzar correlació i anàlisi de *logs*.
CBCS 7 Còpia de seguretat de dades i sistemes	Utilitzar processos i eines per a realitzar la còpia de seguretat de la informació crítica amb una metodologia provada que permeta la recuperació de la informació en temps oportú.	CBCS 7-1: Realització de còpies de seguretat	L'entitat realitza còpies de seguretat automàtiques i periòdicament de totes les dades i configuracions del sistema.
		CBCS 7-2: Realització de proves de recuperació	Es verifica la integritat de les còpies de seguretat realitzades de manera periòdica, i es realitza un procés de recuperació de dades que permeta comprovar que el procés de còpia de seguretat funciona adequadament.
		CBCS 7-3: Protecció de les còpies de seguretat	Les còpies de seguretat es protegeixen adequadament, per mitjà de controls de seguretat física o xifratge, mentre estan emmagatzemades o bé són transmeses a través de la xarxa.
CBCS 8 Compliment normatiu i governança de ciberseguretat	L'entitat compleix els requisits legals i reglamentaris que li són aplicables i té establida una adequada governança de ciberseguretat.	CBCS 8-1: Compliment de l'ENS	L'entitat compleix els requeriments establits en l'ENS.
		CBCS 8-2: Compliment de la LOPD/RGPD	L'entitat compleix els requeriments establits en la LOPD/RGPD.
		CBCS 8-3: Compliment de la Llei 25/2013	L'entitat compleix els requeriments establits en la Llei 25/2013, de 27 de desembre.

Avaluació dels resultats del treball

Els resultats del treball s'analitzen i avaluen a dos nivells: subcontrols i controls.

Subcontrols

Els CBCS són controls globals compostos per diversos controls detallats o subcontrols (tal com es pot veure en el quadre 5 anterior), dels quals hem revisat tant el disseny com l'eficàcia operativa.

El treball d'auditoria consisteix bàsicament a avaluar cada subcontrol en funció dels resultats de les proves realitzades i de les evidències obtingudes. Cada subcontrol s'avalua segons l'escala que es mostra en el quadre següent:

Quadre 6. Avaluació dels subcontrols

Avaluació	Descripció
Control efectiu	Cobreix al 100% l'objectiu de control i: - El procediment està formalitzat (documentat i aprovat) i actualitzat. - El resultat de les proves realitzades per a verificar-ne la implementació i eficàcia operativa ha sigut satisfactori.
Control bastant efectiu	En línies generals, compleix l'objectiu de control, si bé pot haver-hi certs aspectes no coberts al 100% i: - Se segueix un procediment formalitzat, encara que pot presentar aspectes de millora (detall, nivell d'actualització, nivell d'aprovació, etc.). - Les proves realitzades per a verificar la implementació són satisfactòries. - S'han detectat incompliments en les proves realitzades per a verificar l'eficàcia operativa, però no són ni significatius ni generalitzats.
Control poc efectiu	Cobreix de forma molt limitada l'objectiu de control i: - Se segueix un procediment, encara que aquest pot no estar formalitzat. - El resultat de les proves d'implementació i d'eficàcia no és satisfactori. Cobreix en línies generals l'objectiu de control, però: - No se segueix un procediment clar. - Les proves realitzades per a verificar la implementació o l'eficàcia operativa no són satisfactòries (s'han detectat incompliments significatius, encara que no estan generalitzats).
Control no efectiu o no implantat	No cobreix l'objectiu de control. El disseny cobreix l'objectiu de control, però el resultat de la revisió realitzada posa de manifest que la implementació o l'eficàcia operativa del control no són satisfactòries (s'han detectat incompliments significatius i generalitzats).

Controls

Per a determinar la situació global de cada control de ciberseguretat hem utilitzat el **model de nivell de maduresa** dels processos de control d'acord amb el que s'estableix en la GPF-

OCEX 5313, que al seu torn està basada en la *Guia de seguretat CCN-STIC 804* del CCN, usant una escala que es resumeix en el quadre següent.

Quadre 7. Nivells de maduresa

Nivell	Índex	Descripció
N0 Inexistent	0	El control no s'està aplicant en aquest moment.
N1 Inicial / ad hoc	10	El procés existeix, però no es gestiona. L'enfocament general de gestió no és organitzat. *L'organització no proporciona un entorn estable. L'èxit o fracàs del procés depén de la competència i bona voluntat de les persones i és difícil preveure la reacció davant d'una situació d'emergència. En aquest cas, les organitzacions excedeixen amb freqüència pressupostos i temps de resposta. L'èxit del nivell 1 depén de tindre personal d'alta qualitat.*
N2 Repetible, però intuïtiu	50	Els processos segueixen una pauta regular quan determinats procediments es realitzen per diferents persones. No hi ha procediments escrits ni activitats formatives. *L'eficàcia del procés depén de la bona sort i de la bona voluntat de les persones. Existeix un mínim de planificació que proporciona una pauta a seguir quan es repeteixen les mateixes circumstàncies. És impredictible el resultat si es donen circumstàncies noves. Encara hi ha un risc significatiu d'excedir les estimacions de cost i temps.*
N3 Procés definit	80	Els processos estan estandarditzats, documentats i comunicats amb accions formatives. *Es disposa d'un catàleg de processos que es manté actualitzat. Aquests garanteixen la consistència de les actuacions entre les diferents parts de l'organització, que adapten els seus processos particulars al procés general. Hi ha normativa establida i procediments per a garantir la reacció professional davant dels incidents. S'exerceix un manteniment regular. Les oportunitats de sobreviure són altes, encara que sempre queda el factor d'allò desconegut (o no planificat).* *L'èxit és més que bona sort: es mereix.* *Una diferència important entre el nivell 2 i el nivell 3 és la coordinació entre departaments i projectes, coordinació que no existeix en el nivell 2 i que sí que es gestiona en el nivell 3.*
N4 Gestionat i mesurable	90	La direcció controla i mesura el compliment dels procediments i adopta mesures correctores quan es requereix. *Es disposa d'un sistema de mesures i mètriques per a conéixer l'acompliment (eficàcia i eficiència) dels processos. La direcció és capaç d'establir objectius qualitatius i disposa de mitjans per a valorar si s'han aconseguit els objectius i en quina mesura.* *En el nivell 4 de maduresa, el funcionament dels processos està sota control amb tècniques estadístiques i quantitatives. La confiança està quantificada, mentre que en el nivell 3, la confiança era solament qualitativa.*
N5 Optimitzat	100	Se segueixen bones pràctiques en un cicle de millora contínua. *El nivell 5 de maduresa se centra en la millora contínua dels processos amb millores tecnològiques incrementals i innovadores.* *S'estableixen objectius quantitatius de millora, i es revisen contínuament per a reflectir els canvis en els objectius de negoci, utilitzant-se com a indicadors en la gestió de la millora dels processos.* *En aquest nivell l'organització és capaç de millorar l'acompliment dels sistemes a base d'una millora contínua dels processos basada en els resultats de les mesures i indicadors.*

L'avaluació que realitzem sobre el nivell de maduresa no s'ha basat únicament en els processos teòrics o en els procediments aprovats, sinó també en la comprovació de la seua aplicació pràctica.

Per a avaluar el nivell de maduresa de cada control s'han tingut en compte els resultats obtinguts en la revisió dels subcontrols que el formen.

Aquest model proporciona una base sòlida per a formar-se una idea general de la situació en l'entitat revisada en relació amb els controls de ciberseguretat i el compliment de la legalitat en aquesta matèria. També permet comparar resultats entre diferents ens i entre diferents períodes.

Nivell de maduresa mínim requerit en funció de la categoria dels sistemes d'informació auditats

Als sistemes de les tecnologies de la informació i la comunicació dels organismes del sector públic obligats al compliment de l'ENS se'ls assigna una categoria en funció de la valoració de l'impacte que tindria sobre l'organització un incident que afectara la seguretat de la informació o dels sistemes, amb repercussió en la capacitat organitzativa per a:

a) Aconseguir els seus objectius.

b) Protegir els actius al seu càrrec.

c) Complir les seues obligacions diàries de servei.

d) Respectar la legalitat vigent.

e) Respectar els drets de les persones.

A fi de poder determinar l'impacte que tindria sobre l'organització un incident d'aquest tipus, i de poder establir la categoria del sistema, s'han de tindre en compte les **cinc dimensions de la seguretat** que els controls de ciberseguretat han de garantir:

Confidencialitat	És la propietat de la informació per la qual es garanteix que està accessible únicament a personal autoritzat a accedir a aquesta informació.
Integritat	És la propietat de la informació per la qual es garanteix l'exactitud de les dades transportades o emmagatzemades, assegurant que no se n'ha produït l'alteració, pèrdua o destrucció, ja siga de manera accidental o intencionada, per errors de programari o maquinari o per condicions mediambientals.
Disponibilitat	Es tracta de la capacitat d'un servei, un sistema o una informació, de ser accessible i utilitzable pels usuaris o processos autoritzats quan aquests ho requerisquen.

Autenticitat	És la propietat o característica consistent en el fet que una entitat és qui diu ser o bé que garanteix la font de la qual procedeixen les dades.
Traçabilitat	És la propietat o característica consistent en el fet que les actuacions d'una entitat poden ser imputades exclusivament a aquesta entitat.

Una informació o un servei es poden veure afectats en una o més de les seues dimensions de seguretat. Cada dimensió de seguretat afectada s'adscriurà a un dels nivells següents: BAIX, MITJÀ o ALT.

Tenint en compte això, es defineixen tres categories de sistemes d'informació:

a) Un sistema d'informació serà de categoria ALTA si alguna de les seues dimensions de seguretat aconsegueix el nivell ALT.

b) Un sistema d'informació serà de categoria MITJANA si alguna de les seues dimensions de seguretat aconsegueix el nivell MITJÀ, i cap aconsegueix un nivell superior.

c) Un sistema d'informació serà de categoria BÀSICA si alguna de les seues dimensions de seguretat aconsegueix el nivell BAIX, i cap aconsegueix un nivell superior.

La categoria d'un sistema d'informació, en matèria de seguretat, modula l'equilibri entre la importància de la informació que maneja, dels serveis que presta i l'esforç de seguretat requerit, en funció dels riscos a què està exposat, sota el criteri del principi de proporcionalitat.

D'acord amb la categoria de cada sistema, els nivells mínims d'exigència o de maduresa requerits són:[10]

Categoria del sistema	Nivell mínim d'exigència/maduresa requerit
BÀSICA	N2 – Reproduïble, però intuïtiu (50%)
MITJANA	**N3 – Procés definit (80%)**
ALTA	N4 – Gestionat i mesurable (90%)

Els sistemes auditats en aquest informe són considerats a l'efecte de l'ENS com de categoria MITJANA i el nivell de maduresa requerit o objectiu és *N3, procés definit,* i un índex de maduresa del 80%.

Per tant, hem analitzat si els resultats obtinguts d'acord amb el model de nivell de maduresa aconsegueixen el nivell mínim d'exigència requerit en l'ENS, que en aquest cas és *N3, procés definit,* i un índex de maduresa del 80%.

[10] *Guía de seguridad de las TIC. CCN-STIC 824. Informe Nacional del Estado de Seguridad de los Sistemas TIC.*

Indicadors globals

A l'efecte de l'ENS, la guia CCN-STIC-824 preveu una sèrie d'indicadors agregats capaços d'aportar informació resumida sobre l'estat de la seguretat en els organismes públics. Aquests indicadors han sigut adaptats per a la seua aplicació als CBCS, ja que permeten dur a terme un resum de l'estat de les mesures de seguretat dels ens auditats:

- L'**índex de maduresa** sintetitza, en tant per cent, el nivell de maduresa aconseguit per un organisme respecte del conjunt de controls de ciberseguretat.

- L'**índex de compliment** analitza igualment el nivell de maduresa aconseguit, però en relació amb l'exigència aplicable en cada cas, tenint en compte la categoria del sistema. És a dir, compara l'índex de maduresa amb el nivell mínim exigit per a aquesta categoria en l'ENS, que en aquesta auditoria és N3 (80%) per a tots els casos.

Governança de ciberseguretat

A l'efecte d'aquest treball, s'entén per governança de la seguretat de la informació i les comunicacions o de ciberseguretat (termes que utilitzem de manera indistinta en aquest informe) el conjunt de responsabilitats i activitats realitzades per l'alta direcció amb l'objectiu de proporcionar una direcció estratègica en aquesta matèria, garantir que s'aconseguisquen els objectius, verificar que el risc es gestione adequadament i comprovar que s'utilitzen els recursos de l'entitat d'una forma responsable.[11]

Els principals elements d'una adequada governança de ciberseguretat estan implícits en l'ENS i la normativa relativa a la protecció de dades de caràcter personal, normes que revisem en el CBCS 8. Atesa la seua importància nuclear per a la ciberresiliència de l'entitat destaquem de manera explícita la nostra avaluació de la governança existent.

La governança és el procés d'establir i mantindre un marc de referència, i donar suport a l'estructura i els processos de gestió per a garantir la confidencialitat, integritat, disponibilitat, traçabilitat i autenticitat de les dades.

És més que una mera qüestió tècnica, per la qual cosa **exigeix un lideratge efectiu, processos sòlids i estratègies d'acord amb els objectius de l'organització.**[12]

La responsabilitat sobre aquest procés és de l'alta direcció, que, en el cas de les entitats locals, correspon al seu president i a la junta de govern. Ells són els responsables de garantir que el funcionament de l'organització resulta conforme amb les normes aplicables i que hi haja uns controls adequats sobre els sistemes d'informació i les comunicacions. La responsabilitat de l'execució de les activitats establides per l'alta direcció correspon als gestors, a la direcció executiva.

[11] Vegeu el glossari de la Information Systems Audit and Control Association (ISACA).

[12] Vegeu l'apartat 66 d'*Análisis núm. 02/2019: Desafíos de una política eficaz de ciberseguridad en la UE,* del Tribunal de Comptes Europeu.

La implicació dels òrgans superiors és, potser, el factor més important per a la implantació amb èxit d'un sistema de gestió de la seguretat de la informació o de ciberseguretat.[13] L'alta direcció ha de demostrar lideratge i compromís respecte al sistema de gestió de seguretat de la informació,[14] que ha de materialitzar-se en aspectes com ara:

- D'acord amb l'article 11 del Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat, ha de formular-se la **política de seguretat de la informació (PSI) que ha de ser aprovada pel titular de l'òrgan superior** de l'entitat. Aquesta PSI s'ha de difondre entre la totalitat dels membres de l'organització, així com, si és el cas, a proveïdors i tercers.

- Assignar els rols i responsabilitats en matèria de seguretat de la informació. Els òrgans superiors de l'entitat han de nomenar el **responsable de la informació** (que pot tractar-se d'una persona o un òrgan col·legiat), el **responsable del servei** (que pot ser el mateix que l'anterior), el **responsable de la seguretat** i el **responsable del sistema**.

  El procediment de nomenament formal dels responsables esmentats ha de constar en la política de seguretat de la informació de l'entitat.

- Autoritzar la implementació i operació d'un **comité de seguretat TIC**.

  La governança de la seguretat de la informació en una organització s'articula a través d'un comité de seguretat TIC,[15] que es constitueix com un òrgan col·legiat, alguns dels membres del qual exerciran rols especialitzats dins de l'organització de la seguretat, i és la màxima autoritat en l'organització respecte a les decisions de seguretat que afecten els sistemes que manegen informació o presten algun servei. La seua composició ha de constar en la PSI.

- **Proporcionar els recursos materials i humans** necessaris i assegurar que s'implanten programes de conscienciació, formació i capacitació.

  El manteniment actualitzat i la millora dels controls de ciberseguretat requerirà actuacions i inversions, tant en mitjans materials com personals, que han de ser planificades adequadament.

- Decidir els criteris d'acceptació del risc i els nivells acceptables de risc.

- Dirigir les revisions periòdiques de la PSI i vetlar per la realització de les auditories internes de seguretat.

[13] *Guía de iniciación a actividad profesional. Implantación de sistemas de gestión de la seguridad de la información (SGSI) según la norma ISO 27001*, Col·legi Oficial d'Enginyers de Telecomunicació.

[14] *UNE-EN ISO/IEC 27001 Tecnologia de la informació. Tècniques de seguretat. Sistemes de gestió de la seguretat de la informació*, apartat 3.4.

[15] *Guía de seguridad de las TIC, CCN-STIC 201. Organización y gestión para la seguridad de las TIC*, CCN, gener de 2021.

Seguiment de les recomanacions

En aquest treball s'ha realitzat el seguiment de les recomanacions recollides en l'apartat 6 de l'Informe d'auditoria dels controls bàsics de ciberseguretat de l'Ajuntament d'Elx. Exercici 2019.

En la valoració de la situació actual, s'ha seguit la GPF-OCEX 1735, "Les recomanacions i el seu seguiment", que proposa la categorització següent:

Quadre 8. Situació de les recomanacions

Totalment o substancialment aplicada	Si l'ens fiscalitzat ha adoptat les mesures correctores, raonables i proporcionades en l'esfera de les seues competències, que permeten considerar que la recomanació ha produït efectes i no ha quedat pendent de resolució cap qüestió d'importància significativa. En aquests casos s'entendrà que la recomanació s'ha complit raonablement. A més, s'ha obtingut evidència suficient que acredita les mesures adoptades.
Aplicada parcialment	Si l'ens fiscalitzat ha pres en consideració les recomanacions i ha realitzat actuacions encaminades a corregir les deficiències, debilitats o insuficiències que s'han posat de manifest, però solament en un estat incipient, en una part o en alguns aspectes, la qual cosa no permet considerar que la recomanació s'ha complit raonablement.
No aplicada	Si l'ens fiscalitzat no ha realitzat les actuacions encaminades a corregir les deficiències, debilitats o insuficiències que s'han posat de manifest o bé ho ha fet insuficientment o inadequadament de manera que la recomanació segueix sense aplicar-se.
Sense validesa en el marc actual	S'hi inclouen les recomanacions que, encara que vàlides i pertinents quan es va emetre l'informe i per a l'exercici fiscalitzat, i fins i tot sent acceptades i reconegudes per l'ens fiscalitzat, no poden aplicar-se en el context actual perquè no es donen les circumstàncies que ho permeten o la mateixa casuística que llavors, és a dir, no es donen en el moment actual els supòsits dels fets en funció dels quals es va efectuar la recomanació en el passat. La recomanació ha esdevingut inaplicable.
No verificada	S'inclouen en aquesta categoria les recomanacions que, encara que acceptades o fins i tot aplicades i corregides per l'ens fiscalitzat, necessitarien obligatòriament alguna prova addicional per a contrastar el que ha manifestat l'ens fiscalitzat que excedeixen l'abast previst en el treball.

En el quadre 2 es mostren les recomanacions contingudes en l'informe esmentat amb els comentaris relatius al seguiment realitzat i la situació a 31 de desembre de 2021.

Comunicació i confidencialitat

Ens comuniquem amb els responsables de l'entitat en relació, entre altres qüestions, amb l'abast i el moment de realització de l'auditoria planificats i les constatacions significatives de l'auditoria, com també amb qualsevol deficiència significativa dels controls interns que identifiquem en el transcurs de l'auditoria.

Atés que la informació utilitzada en l'auditoria té un caràcter sensible i pot afectar la seguretat dels sistemes d'informació, els resultats amb el màxim detall de cada un dels

controls revisats només es comuniquen amb caràcter confidencial als responsables de l'Ajuntament perquè puguen adoptar les mesures correctores que consideren necessàries. En aquest informe els resultats es mostren de manera sintètica.

APÈNDIX 2
Situació dels controls bàsics de ciberseguretat

CBCS 1. INVENTARI I CONTROL DE DISPOSITIUS FÍSICS

Objectiu del control

Gestionar activament (inventariar, revisar i corregir) els dispositius físics connectats en la xarxa, de manera que només els dispositius autoritzats tinguen accés a la xarxa.

Situació del control

L'Ajuntament no ha elaborat un procediment que definisca les accions necessàries per a mantindre controlat i actualitzat l'inventari de dispositiu de maquinari. L'inventari integral de l'entitat està format pels inventaris mantinguts en els diferents departaments.

L'eina utilitzada pel departament d'informàtica per a l'inventari de maquinari continua sent OCS Inventory, vista en l'auditoria anterior. No obstant això, una de les millores implantades per part del departament d'informàtica ha sigut l'eina Cytomic EPDR, que mostra l'inventari dels actius físics que tenen l'agent de xarxa instal·lat i que ha sigut desplegada en totes les àrees de l'Ajuntament. Encara que l'objectiu principal de l'eina no és l'inventari d'actius, permet comprovar l'estat dels equips amb agent de xarxa. El departament d'informàtica es troba en fase de proves de la característica que té Cytomic per al control de dispositiu de maquinari.

Per a l'electrònica de xarxa, el departament de telecomunicacions es troba en 2022 en fase d'actualització de tots els *switches*. Encara que el treball no ha finalitzat, l'electrònica ja ha sigut completament renovada en algunes dependències. Aquest canvi suposa una millora significativa en la gestió de tota l'electrònica de xarxa, centralitzant el control dels sistemes per mitjà de l'eina Identity Services Engine (ISE) de Cisco. Aquest departament continua gestionant els inventaris manuals ja esmentats en l'auditoria anterior.

El departament de policia gestiona el seu propi inventari d'actiu de maquinari de manera manual, per mitjà de l'eina de gestió policial i, com a millora, s'han afegit els seus equips client al programari de Cytomic gestionat per informàtica.

Per a impedir l'accés a la xarxa corporativa de dispositius no autoritzats, el departament de telecomunicacions, a més dels controls vistos en l'auditoria anterior, es troba en fase d'implantació d'un sistema de control d'accés a la xarxa (NAC*, network access control*), desplegat en tres edificis i l'objectiu del qual és implantar-lo en la totalitat de les dependències de l'entitat. El sistema NAC té catalogades les direccions físiques (MAC*, media access control)* dels dispositius autoritzats i impedeix a qualsevol altre dispositiu navegar fora de la xarxa de convidats. Si la direcció MAC està dins del conjunt de direccions autoritzades, se sol·licita credencials del domini a l'usuari i es deriva l'usuari a la subxarxa pertinent d'acord amb els permisos del directori actiu.

La valoració global del control és que l'Ajuntament aconsegueix un **índex de maduresa del 45,0%**, que es correspon amb un **nivell de maduresa *N1*, *inicial/ad hoc***; és a dir, el

procés existeix, però no es gestiona o la gestió no està organitzada correctament. Això representa un **índex de compliment del CBCS 1 del 56,3%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 34,8%, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una millora de 10,2 punts en l'índex de maduresa del control.

CBCS 2. INVENTARI I CONTROL DE PROGRAMARI AUTORITZAT

Objectiu del control

Gestionar activament (inventariar, revisar i corregir) tot el programari en la xarxa, de manera que només es puga instal·lar i executar programari autoritzat i que el no autoritzat siga detectat i se n'evite la instal·lació i execució.

Situació del control

L'Ajuntament no disposa de procediment aprovat per a la gestió integral del programari de l'entitat.

Hi ha diferents inventaris que formen l'inventari de programari de l'entitat. D'una banda, l'inventari d'OCS Inventory, complet i que afecta tots els actius de l'entitat amb agent de xarxa. D'una altra, la nova eina Cytomic EPDR manté un inventari centralitzat del programari instal·lat en els actius que disposen d'agent de xarxa.

L'Ajuntament té implantades algunes mesures que garanteixen cert nivell de control sobre el programari de l'entitat, com l'ús d'usuaris sense privilegis d'administració, l'actualització de gran part dels sistemes que estaven fora de suport vistos durant l'auditoria anterior o l'activació d'un control d'aplicacions en el programari Cytomic. No obstant això, es mantenen les nostres recomanacions atés que:

- No hi ha una política de gestió de programari formalment aprovada.
- No hi ha revisions periòdiques del programari instal·lat.
- Les mesures que permeten bloquejar aplicacions no autoritzades són limitades i millorables.
- No hi ha un pla de manteniment de programari.
- Hi ha sistemes fora del seu període de suport.

La valoració global del control és que l'Ajuntament aconsegueix un **índex de maduresa del 56,5%**, que es correspon amb un **nivell de maduresa *N2*, *repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 2 del 70,6%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 49,0%, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una millora de 7,5 punts en l'índex de maduresa del control.

CBCS 3. PROCÉS CONTINU D'IDENTIFICACIÓ I SOLUCIÓ DE VULNERABILITATS

Objectiu del control

Disposar d'un procés continu per a obtindre informació sobre noves vulnerabilitats, identificar-les, remeiar-les i reduir la finestra d'oportunitat als atacants.

Situació del control

L'Ajuntament continua sense un procediment aprovat per a la gestió de vulnerabilitats que definisca les accions dutes a terme per a la identificació, anàlisi, priorització, seguiment i resolució d'aquestes en dispositius, sistemes i aplicacions.

Una de les millores significatives en aquest control ha sigut la implantació, per part del departament d'informàtica, de l'eina Cytomic EPDR esmentada anteriorment i l'assignació de personal tècnic a aquest efecte. Per mitjà del mòdul Cytomic Patch, el departament gestiona les actualitzacions i pedaços dels sistemes amb agent de xarxa instal·lat, incloent-hi les actualitzacions de les aplicacions instal·lades en aquests equips. Encara que l'agent de xarxa està desplegat en tots els equips de l'entitat, el departament d'informàtica únicament gestiona les vulnerabilitats sobre els equips de la seua competència i en els equips de telecomunicacions, mentre que la policia fa la seua pròpia gestió de pedaços i actualitzacions dels sistemes operatius dels seus equips.

Per mitjà de la consola centralitzada s'identifiquen vulnerabilitats atenent la seua criticitat, i els pedaços i actualitzacions es despleguen de manera automatitzada periòdicament. El departament d'informàtica ha contractat un servei estés de suport de Cytomic que inclou revisions periòdiques al panell, a més de la implantació de millores i resolució d'incidències.

El departament de policia actualitza els seus equips per mitjà de directives de grup del directori actiu. No hem revisat amb quina periodicitat s'instal·len o si el departament realitza revisions periòdiques de programari per a verificar la correcta actualització d'equips i aplicacions.

El departament de telecomunicacions està substituint els *switches* en tota la xarxa corporativa. Actualment ja s'han actualitzat els *switches* dels primers edificis. La nova electrònica disposa d'una consola d'administració del fabricant que permet fer-ne la gestió centralitzadament, incloent-hi el desplegament d'actualitzacions i pedaços.

Addicionalment, des del departament de telecomunicacions, en col·laboració amb el departament d'informàtica, s'ha dut a terme el desplegament de la solució del CCN microCLAUDIA en tots els equips de la xarxa.

Encara que s'ha millorat el control per a la gestió de vulnerabilitats, continua havent-hi possibilitats de millora que garantirien major efectivitat, com l'ús d'eines d'escaneig de vulnerabilitats, auditories de *hacking* ètic o la documentació de les accions dutes a terme des de la identificació fins a la resolució de vulnerabilitats crítiques. A més, és necessari que s'aprove un procediment que preveja aquestes accions i s'aplique d'igual manera a tots els sistemes de l'entitat.

La valoració global del control és que l'Ajuntament aconsegueix un **índex de maduresa del 54,8%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 3 del 68,4%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 27,6%, que es correspon amb un nivell de maduresa *N1, inicial/ad hoc*. Per tant, s'ha produït una notable millora de 27,2 punts en l'índex de maduresa del control. Les accions en marxa permetran millorar l'eficàcia d'aquest control.

CBCS 4. ÚS CONTROLAT DE PRIVILEGIS ADMINISTRATIUS

Objectiu del control

Desenvolupar processos i utilitzar eines per a identificar, controlar, previndre i corregir l'assignació i ús de privilegis administratius en els sistemes d'informació.

Situació del control

Encara que l'Ajuntament ha realitzat algunes accions per a millorar les deficiències en la gestió de comptes amb privilegis d'administració, aquestes accions no es troben establides en un procediment formalment aprovat, ni s'apliquen de manera homogènia a tots els dispositius, sistemes i aplicacions de l'entitat. Continua existint una gestió diferent en cada un dels tres departaments analitzats, sense un procediment únic que governe d'igual manera tota l'organització.

L'Ajuntament ha de continuar millorant la gestió dels privilegis administratius per mitjà de:

- Aprovació d'un procediment unificat que definisca la gestió d'usuaris amb privilegis administratius, que incloga l'alta, baixa i revisió periòdica d'usuaris, de manera que totes les aplicacions i sistemes tinguen actualitzats els usuaris actius de l'entitat. El procediment ha d'incloure la revisió periòdica d'usuaris i perfils sobre totes les aplicacions de l'entitat, incloent-hi comptabilitat i recaptació, i les accions a auditar dels usuaris amb perfils d'administració sobre dispositius i sistemes crítics.

- Encara que s'han revisat i eliminat els usuaris no nominatius amb permisos d'administració en alguns dels sistemes, com l'electrònica de xarxa nova, el sistema de virtualització utilitzat en telecomunicacions, el directori actiu o les aplicacions de gestió

del departament d'informàtica, continua havent-hi administradors no nominatius en alguns dels sistemes revisats.

- Establir, per als administradors de sistemes, diferents usuaris amb diferents nivells de privilegis i utilitzar-los en funció de les tasques a realitzar. S'ha verificat que el departament d'informàtica està realitzant proves respecte a aquest punt.

- Aprovació d'una política de contrasenyes d'aplicació homogènia a tots els sistemes de l'entitat. Existeix un esborrany ja elaborat d'aquesta política pendent d'aprovació.

La valoració global del control és que l'Ajuntament aconsegueix un **índex de maduresa del 45,2%**, que es correspon amb un **nivell de maduresa *N1*, *inicial/ad hoc***; és a dir, el procés existeix, però no es gestiona o la gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 4 del 56,5%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 29,9%; per tant, s'ha produït una millora de 15,3 punts en l'índex de maduresa del control.

CBCS 5. CONFIGURACIONS SEGURES DEL PROGRAMARI I MAQUINARI

Objectiu del control

Establir una configuració base segura del programari i maquinari de dispositius mòbils, portàtils, equips de taula i servidors, i gestionar-la activament, utilitzant un procés de gestió de canvis i configuracions rigorós, per a previndre que els atacants exploten serveis i configuracions vulnerables.

Situació del control

Hem analitzat les accions dutes a terme per l'Ajuntament per al control de configuracions de dispositius i sistemes i hem verificat que no hi ha un procés formalment establit a aquest efecte.

El departament d'informàtica ha implantat, per mitjà de l'eina Cytomic Encriptation, una mesura que permet encriptar la informació dels ordinadors portàtils. No obstant això, aquesta mesura no es troba aplicada en tots els equips ni està establida en cap procediment.

A més de l'eina anterior, el departament utilitza l'eina PRTG per a monitorar l'estat dels servidors que gestiona.

Per la seua banda, el departament de telecomunicacions ha realitzat determinades accions encaminades a millorar la fortificació dels seus sistemes, com l'ús de l'eina del CCN Rocio per a elaborar les plantilles de l'electrònica de xarxa nova, la gestió centralitzada de l'electrònica de xarxa nova, o la licitació d'un contracte que inclou una auditoria de la infraestructura de xarxa per a adoptar totes les mesures que siguen necessàries per a donar compliment a les normatives i recomanacions de seguretat de l'ENS.

Si bé la policia ja va evidenciar l'ús de plantilles i configuracions basades en les guies STIC, no s'han aportat millores sobre aquest tema.

Encara que l'Ajuntament ha realitzat les accions anteriors per a millorar la seguretat de dispositius i aplicacions, continua havent-hi deficiències en els aspectes que s'enumeren a continuació:

- No hi ha procediments formalment aprovats l'objecte dels quals siga la configuració segura de dispositius, que incloguen les pautes i recomanacions dels fabricants o de les institucions de referència en matèria de seguretat.

- No es disposa d'un procediment de gestió de canvis per a sistemes crítics de l'entitat que descriga les accions que cal realitzar per a fer canvis en aquests sistemes, que els monitore i que alerte de canvis no autoritzats.

Existeix un insuficient nivell de control sobre les configuracions segures en dispositius i sistemes i la valoració de l'**índex de maduresa és del 43,2%**, que es correspon amb un **nivell de maduresa *N1, inicial/ad hoc***; és a dir, el procés existeix, però no es gestiona o la gestió no està correctament organitzada. Això representa un **índex de compliment del CBCS 5 del 54,0%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 30,0%. Per tant, s'ha produït una millora de 13,2 punts en aquest índex.

CBCS 6. REGISTRE DE L'ACTIVITAT DELS USUARIS

Objectiu del control

Recollir, gestionar i analitzar els registres d'esdeveniments que poden ajudar a detectar, entendre o recuperar-se d'un atac.

Situació del control

L'Ajuntament ha realitzat determinats canvis per a millorar el control sobre el registre de l'activitat dels usuaris en els diferents sistemes; no obstant això, les accions i eines implantades continuen sense establir-se en un procediment formalment aprovat.

El departament d'informàtica ha implantat una eina SIEM per al registre de *logs* d'auditoria i anàlisi d'amenaces de seguretat, que inclou un analitzador de *logs* per als equips d'usuari i els servidors de fitxers que alberguen les carpetes compartides. Encara que la implantació d'aquesta eina és una millora substancial per al control sobre el registre d'accions dels usuaris i la seguretat del sistema d'informació, el departament n'ha d'optimitzar la configuració de manera que maximitze la qualitat de la informació aportada.

El departament de policia, per la seua banda, ha activat per mitjà de directives de grup del directori actiu el *log* en tots els equips d'usuari. Aquest *log* és exportat a una base de dades i no es revisa regularment, sinó que es guarda a l'efecte d'investigació d'incidents.

Finalment, el departament de telecomunicacions afirma no haver fet canvis organitzatius o tècnics respecte a la situació observada en l'auditoria anterior, encara que afirma trobar-se en fase de contractació de serveis que inclouen aspectes relacionats amb aquest control.

Encara que s'han realitzat accions que milloren el control sobre els registres d'activitat dels usuaris, és necessari que la corporació definisca i aprove un procediment per a la gestió dels registres d'activitat, en què es descriga quines accions i sobre quins sistemes és necessari realitzar un registre d'activitat, durant quant de temps es guarden, qui són els responsables, periodicitat de les revisions, mecanismes per a impedir modificacions en els registres o còpia de seguretat d'aquests.

Hi ha cert nivell de control sobre el registre d'activitat dels usuaris, i la nostra valoració mostra un **índex de maduresa del 56,5%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 6 del 70,6%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 53,0%, per tant, s'ha produït una lleu millora de 3,5 punts en l'índex de maduresa del control.

CBCS 7. CÒPIA DE SEGURETAT DE DADES I SISTEMES

Objectiu del control

Utilitzar processos i eines per a realitzar la còpia de seguretat de la informació crítica amb una metodologia provada que permeta recuperar la informació en temps oportú.

Situació del control

L'Ajuntament no ha desenvolupat una política que establisca les accions que s'han d'executar sobre les còpies de seguretat, que definisca els sistemes i dades que cal protegir, i incloga aspectes com la periodicitat, responsables, mesures de protecció, proves de restauració planificades, etc.

Encara que existeix cert nivell de control sobre les còpies, són els màxims responsables de l'entitat els qui han de decidir la informació crítica que cal protegir i elaborar les pautes per a totes les àrees de l'entitat. La inexistència d'una política unificada de còpies que s'aplique a tota l'entitat fa que cada un dels departaments gestione les còpies de manera diferent i amb diferents criteris.

El departament d'informàtica ha millorat el sistema de còpies per mitjà de l'activació dels *snapshots* en els sistemes Windows. En 2022, i per tant no avaluat en aquest informe, el departament ha implantat l'eina Veeam Backup per a la gestió de les seues còpies de seguretat.

L'àrea de policia realitza diferents accions per al control sobre les còpies de seguretat: còpies de fitxers, bases de dades, servidors, etc. Hi ha dos nivells de còpies desconnectades, un NAS (*network attached storage,* dispositiu d'emmagatzematge connectat a la xarxa) únicament accessible des d'una adreça IP habilitada i còpies externes cada dos dies guardades en una caixa de seguretat. Addicionalment, tenen programat un *script* que avisa per Telegram de l'estat de les còpies. No obstant això, tot el procés es realitza de manera manual per mitjà de *scripts* i és dependent de la voluntat dels responsables perquè no es recull en un procediment aprovat formalment.

El departament de telecomunicacions, per la seua banda, realitza les còpies de seguretat dels servidors per mitjà del programari Veeam Backup. Pel que fa a la nova electrònica de xarxa, com que permet la gestió de manera centralitzada, és altament recomanable realitzar còpies de seguretat del microprogramari dels dispositius que gestiona, així com de la consola d'administració, encara que hi ha controls compensatoris com la còpia del servidor complet que alberga aquesta consola.

Cap dels tres departaments realitza proves planificades periòdiques de recuperació de sistemes crítics des de les còpies de seguretat. No obstant això, el departament d'informàtica sí que realitza anualment una restauració completa d'un dels seus sistemes crítics, l'AS400.

La deficiència més significativa és la falta d'un procediment o política de còpies de seguretat aprovada per la corporació i que s'aplique de manera homogènia a totes les àrees de l'entitat i definisca les dades que cal protegir, els responsables, la periodicitat, proves de restauració planificades, temps de recuperació i la seguretat de les còpies.

La valoració global del control és que l'Ajuntament aconsegueix un **índex de maduresa del 61,5%**, que es correspon amb un **nivell de maduresa *N2, repetible però intuïtiu***; és a dir, els controls es realitzen, però hi ha controls parcialment establits o els procediments no s'han formalitzat documentalment. Això representa un **índex de compliment del CBCS 7 del 76,9%**.

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 66,5%. La raó del descens és que en 2019 no es van avaluar alguns aspectes sobre les còpies en la policia, que té establit un procés de còpies manual per mitjà de *scripts* que, encara que és parcialment efectiu, no segueix directrius aprovades per la corporació a aquest efecte, no es gestionen de manera centralitzada ni el procés és sistemàtic i depén de la bona voluntat dels responsables. Aquests motius fan que s'haja produït un decrement de 5 punts en l'índex de maduresa del control.

CBCS 8. COMPLIMENT NORMATIU I GOVERNANÇA DE CIBERSEGURETAT

Objectiu del control

Assegurar el compliment de la normativa bàsica en matèria de seguretat de la informació, la qual cosa inclou l'establiment d'una adequada governança de ciberseguretat.

Situació del control

Compliment de l'ENS

L'Ajuntament, des de l'auditoria realitzada l'any 2019, no ha realitzat les correccions proposades per a complir el que es preveu en el Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica.

Encara que l'Ajuntament ha dut a terme algunes accions encaminades al compliment de l'ENS, com ara accions formatives, reunions a fi d'implantar les mesures de seguretat exigides per la normativa, o la inclusió d'aspectes relacionats amb el compliment de l'ENS en els sistemes de telecomunicacions, no s'ha desenvolupat una declaració d'aplicabilitat ni s'han realitzat les auditories pertinents.

Compliment de l'RGPD

L'Ajuntament no ha aprovat el registre d'activitats de tractament ni ha realitzat l'anàlisi de riscos o les auditories requerides per l'RGPD.

Compliment de la legalitat del registre de factures

L'Ajuntament no ha realitzat l'auditoria de sistemes del registre de factures exigida per la Llei 25/2013, de 27 de desembre.

Indicadors

En resum, la valoració global sobre el compliment dels aspectes de legalitat inclosos en la revisió és que l'Ajuntament aconsegueix un **índex de maduresa del 40,0%**, que es correspon amb un **nivell de maduresa N1, que indica que hi ha incompliments significatius generalitzats de la normativa que s'han de solucionar de manera urgent.**

La situació del control en l'informe realitzat l'any 2019 mostrava un índex de maduresa del 35,0%, que es correspon amb un nivell de maduresa *N1*. Per tant, s'ha produït una millora de 5 punts en l'índex de maduresa del control.

Governança de ciberseguretat

L'Ajuntament d'Elx no té establida una governança adequada de la seguretat de la informació.

Els òrgans superiors de l'Ajuntament (alcalde i Junta de Govern) són els responsables que hi haja uns controls adequats sobre els sistemes d'informació i les comunicacions, i la seua implicació, compromís i lideratge constitueixen, possiblement, el factor més important per a la implantació reeixida d'un sistema de gestió de la seguretat de la informació que garantisca la ciberresiliència de l'entitat.

Si bé en l'auditoria hem observat l'existència d'un cert nivell de compromís i conscienciació amb la ciberseguretat per part dels gestors i responsables de les àrees implicades, **hi ha mancances rellevants que indiquen que la governança i nivell de compromís i**

conscienciació amb la ciberseguretat per part dels òrgans superiors de l'Ajuntament és insuficient. Les mancances més rellevants identificades, que dificulten l'establiment d'un sistema de gestió de la seguretat de la informació (SGSI) efectiu, són les següents:

- La falta d'un marc normatiu i procedimental formalment aprovat, que desenvolupe la PSI,[16] inclosa la inexistència de procediments de seguretat formalment assumits per l'organització i que s'apliquen de manera homogènia a totes les seues àrees.

- La participació activa del comité de seguretat de la informació. El comité, òrgan imprescindible per a coordinar la seguretat de la informació en l'entitat i que inclou representació de les àrees de l'organització afectades, ha de reunir-se amb major periodicitat, ja que en 2021 només s'ha reunit una vegada, i tindre un caràcter proactiu en la presa de totes les decisions que afecten la seguretat de la informació, comptant amb els tècnics responsables.

- La inexistència d'una governança adequada implica que, en la pràctica, són els tècnics dels diferents departaments o les empreses adjudicatàries els qui adopten decisions sobre determinats aspectes en matèria de ciberseguretat atenent els seus propis criteris, sense la participació activa del comité de seguretat.

Resulta, per tant, necessària la solució urgent de les mancances identificades, atés que tenen un impacte negatiu en el nivell de seguretat de la corporació. En aquest sentit, els òrgans de govern tenen la responsabilitat de liderar i ser exemplaritzants en les seues accions i decisions, com a part d'un procés de conscienciació de l'entitat.

[16] Segons el CCN, en *Aproximación al marco de gobernanza de la ciberseguridad*, "la importància cabdal de la política de seguretat de la informació, com a base essencial per a la construcció de la seguretat de la informació, fa que constituïsca sempre el primer element que s'ha d'escometre, i ha de ser públicament aprovada pel seu òrgan directiu, com a evidència del **compromís** de l'organització amb la seguretat de la informació i el seu manteniment".

APÈNDIX 3
Bones pràctiques destacables

Introducció

Amb caràcter general, si una entitat aconsegueix una valoració del 80% en l'índex de maduresa d'un control significa que està aplicant de manera raonable les bones pràctiques en matèria de seguretat de la informació establides en l'ENS o en les guies professionals corresponents, que se sintetitzen en el quadre 5 d'aquest informe. En un altre cas, l'entitat ha d'adoptar mesures per a millorar la seua ciberseguretat i aconseguir aquesta meta.

Addicionalment a la valoració dels controls bàsics de ciberseguretat, és convenient destacar determinats aspectes, pràctiques, solucions tècniques o sistemes que s'han identificat o revisat durant la realització de l'auditoria i que destaquen en relació amb l'estat de l'art sobre una determinada matèria. Aquests aspectes proporcionen, per la seua singularitat, un coneixement addicional que facilita la interpretació, contextualització i avaluació dels resultats obtinguts en els procediments d'auditoria per a la valoració dels controls.

A més, atés el caràcter positiu dels aspectes considerats en aquest apartat, la seua identificació pot, en determinats casos, constituir la base de sinergies entre administracions públiques de la mateixa naturalesa i amb característiques similars, ja que es poden reproduir si es donen necessitats i problemàtiques comunes.

El criteri per a determinar si un aspecte és considerat bona pràctica destacable és l'existència d'una o diverses de les circumstàncies següents:

- solucions o sistemes especialment avançats o efectius des del punt de vista tecnològic,
- processos de gestió particularment madurs, i
- solucions o processos poc freqüents entre les entitats auditades, però de demostrada eficàcia davant de les necessitats de l'entitat, independentment de la seua complexitat o innovació.

Els aspectes destacats a continuació, en general, s'han considerat en l'avaluació dels CBCS. No obstant això, alguns no formen part dels CBCS tal com estan definits en la GPF-OCEX 5313, però els comentem per les raons indicades abans. Cal aclarir que l'existència d'aspectes concrets particularment rellevants no implica necessàriament que el control global dispose de la maduresa requerida, ja que la seua valoració inclou la consideració d'un conjunt d'aspectes tècnics, organitzatius i formals que s'han d'aconseguir individualment i en conjunt, amb un determinat nivell d'efectivitat i maduresa.

Sistema de control d'accés a la xarxa (NAC, network access control)

Per a millorar els controls sobre la connexió de dispositius no autoritzats a la xarxa corporativa, a data d'aquest informe, l'Ajuntament es troba en fase de desplegament de mesures que garantisquen l'efectivitat del control.

D'una banda, el departament de telecomunicacions es troba en procés d'actualització de tots els *switches*. Aquesta millora inclou la integració de l'electrònica de xarxa en un sistema de control d'accés a la xarxa corporativa (NAC*, network access control*) que inclou una

consola de gestió centralitzada dels dispositius. El sistema manté una llista de les direccions MAC de tots els dispositius de confiança i aïlla en una subxarxa qualsevol dispositiu que no estiga donat d'alta en aquesta llista. Si el dispositiu és de la llista de direccions de confiança, per mitjà de credencials del domini se situa el dispositiu en la subxarxa corresponent.

Per a garantir l'efectivitat del control, és necessari que les mesures descrites s'apliquen per igual a tots els edificis i departaments de l'organització.

Millora en les instal·lacions físiques

Fruit de les necessitats de substituir un dels CPD de l'entitat que havia quedat obsolet, l'Ajuntament va licitar el projecte per al nou centre de dades.

Entre els requisits establits per a la nova infraestructura hi havia l'estudi tècnic d'emplaçament entre diverses ubicacions, facilitat d'accés, no ocupar massa espai, així com comptar amb un sistema robust de protecció contra factors meteorològics (sismes, inundacions, etc.).

L'empresa adjudicatària va proposar la solució d'un *container datacenter*, és a dir, un contenidor que alberga diferents armaris *rack* organitzats en corredors amb accessos independents. Aquesta solució permet les funcionalitats d'un CPD convencional reduint l'espai i els costos, a més de ser flexibles quant a equipament i configuració.

El projecte ha sigut premiat en la XIII Edició dels Premis ASLAN sobre Digitalització en les Administracions Públiques celebrats en 2021.

ACRÒNIMS I GLOSSARI DE TERMES

CBCS: Controls bàsics de ciberseguretat

CCN: Centre Criptològic Nacional

CGTI: Controls generals de tecnologies de la informació

ENS: Esquema Nacional de Seguretat

INES: Informe Nacional de l'Estat de la Seguretat

LOPD: Llei Orgànica de Protecció de Dades de Caràcter Personal

PSI: Política de seguretat de la informació

RGPD: Reglament General de Protecció de Dades

SGSI: Sistema de gestió de seguretat de la informació

SIC: Sistemes d'informació i comunicacions

Alta direcció: A l'efecte d'aquest treball, ens referim als òrgans superiors de l'Ajuntament (en particular, l'alcalde o l'alcaldessa i la Junta de Govern). Són els responsables que hi haja uns controls adequats sobre els sistemes d'informació i les comunicacions i una adequada governança de ciberseguretat.

Ciberamenaces: Esdeveniments amb origen en internet que poden desencadenar un incident en l'organització i produir danys materials, pèrdues immaterials en els seus actius o la interrupció d'un servei.

Ciberhigiene: Conjunt de pràctiques i accions bàsiques que una organització ha d'implantar per a fer front als riscos de ciberseguretat més comuns i generalitzats als quals s'enfronta hui dia. A l'efecte d'aquest treball, aquest conjunt de pràctiques i accions bàsiques són els CBCS.

Ciberresiliència: És la capacitat d'un procés, negoci, organització o nació per a anticipar, resistir, recuperar-se i evolucionar per a millorar les seues capacitats davant de condicions adverses, estrés o atacs als recursos cibernètics que necessiten per a funcionar. En l'àmbit concret del sector públic, és la capacitat d'un ens públic per a evitar o resistir i recuperar-se d'un atac i continuar prestant els seus serveis en un temps raonable.

Ciberseguretat: És la capacitat de les xarxes o dels sistemes d'informació de resistir, amb un determinat nivell de confiança, els accidents o accions il·lícites o malintencionades que comprometen la disponibilitat, autenticitat, integritat i confidencialitat de les dades

emmagatzemades o transmeses, així com dels serveis que aquestes xarxes i sistemes ofereixen o fan accessibles.

Correlador d'esdeveniments: Correlar és el procés de comparar diferents fonts d'informació d'esdeveniments, donant d'aquesta manera sentit a esdeveniments que, analitzats per separat, no en tindrien o passarien desapercebuts. Un SIEM *(security information and event management)* o sistema de gestió d'informació i esdeveniments de seguretat, va un pas més enllà de les capacitats de monitoratge, emmagatzematge i interpretació de les dades rellevants per mitjà de tècniques de correlació complexa d'esdeveniments.

Direcció: Són els responsables de l'execució de les activitats establides per l'alta direcció en matèria de ciberseguretat, és la direcció executiva. En aquest grup, a l'efecte d'aquest informe, s'inclou el regidor responsable dels sistemes d'informació i les comunicacions, el secretari general, l'interventor general, i els funcionaris directors del departament TIC i els caps d'àrea o servei.

Governança de ciberseguretat: Segons el Tribunal de Comptes Europeu, la governança de la seguretat de la informació consisteix en la creació d'estructures i polítiques per a garantir la confidencialitat, integritat i disponibilitat de les dades. És més que una mera qüestió tècnica, per la qual cosa exigeix un lideratge efectiu, processos sòlids i estratègies d'acord amb els objectius de l'organització. Als efectes d'aquest informe li donem el mateix significat que a *governança de la seguretat de la informació*.

Normes de seguretat: Uniformen l'ús d'aspectes concrets del sistema, indiquen l'ús correcte i les responsabilitats dels usuaris. Són de caràcter obligatori i descriuen: *a*) l'ús correcte d'equips, serveis i instal·lacions; *b*) el que es considerarà ús indegut, i *c*) la responsabilitat del personal respecte al compliment o violació d'aquestes normes. La normativa de seguretat estarà a la disposició de tots els membres de l'organització que necessiten conéixer-la, en particular per a aquells que utilitzen, operen o administren els sistemes d'informació i comunicacions; com a regla general, estarà disponible en la intranet corporativa de l'entitat a través d'una adreça URL. La normativa de seguretat de cada entitat deriva i rep la seua autoritat executiva del que es preceptua en l'ENS, en primera instància, i del desenvolupament normatiu de la política de seguretat de l'entitat en qüestió, en segona instància.

Política de seguretat de la informació: És un document d'alt nivell que defineix el que significa *seguretat de la informació* en una organització d'acord amb l'article 11 del Reial Decret 3/2010 i articula la gestió continuada de la seguretat. Ha de ser aprovada pel president o presidenta o la junta de govern d'una entitat local o el consell d'administració d'una societat. Ha d'estar accessible per a tots els membres de l'organització i redactada de manera senzilla, precisa i comprensible. Convé que siga breu, i que deixe els detalls tècnics per a altres documents més precisos que ajuden a dur a terme el que es proposa: normes de seguretat i procediments de seguretat.

Procediments de seguretat: Aborden tasques concretes i indiquen què cal fer, pas a pas. Detallen de manera clara i precisa: *a*) com dur a terme les tasques habituals, *b*) qui ha de fer cada tasca i *c*) com identificar i reportar comportaments anòmals.

Sistema de gestió de seguretat de la informació: Un SGSI és un enfocament sistemàtic per a establir, implementar, operar, monitorar, revisar, mantindre i millorar la seguretat de la informació d'una organització i aconseguir els seus objectius.

TRÀMIT D'AL·LEGACIONS

Prèviament al tràmit d'al·legacions i segons el que preveu la secció 1220 del *Manual de fiscalització* de la Sindicatura, un esborrany previ de l'Informe d'auditoria es va discutir, amb els interlocutors de les àrees d'informàtica, policia local i telecomunicacions, juntament amb el regidor d'Innovació, Recursos Humans i Seguretat i el secretari general, perquè en tingueren coneixement i per tal que, si era cas, hi efectuaren les observacions que estimaren pertinents.

Posteriorment, en compliment de l'article 16 de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, i de l'article 55.1.*c* del Reglament de Règim Interior de la Sindicatura de Comptes, així com de l'acord del Consell d'aquesta institució pel qual va tindre coneixement de l'esborrany de l'informe d'auditoria corresponent a 2021, aquest es va trametre al comptedant per tal que, en el termini concedit, hi formulara al·legacions.

Transcorregut aquest termini no s'han rebut al·legacions.

APROVACIÓ DE L'INFORME

En compliment de l'article 19.*j* de la Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes, i de l'article 55.1.*h* del seu Reglament de Règim Interior i dels programes anuals d'actuació de 2021 i 2022 d'aquesta institució, el Consell de la Sindicatura de Comptes, en la reunió del dia 7 de setembre de 2022, va aprovar aquest informe d'auditoria.

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

NIF: S9600001C

Document sota custòdia en Seu Electrònica

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA

Informe seguiment recomanacions CBCS Ajuntament Elx de l'any 2019 - SEFYCU 3486703

Podeu accedir a aquest document en format PDF-PAdES i comprovar la seua autenticitat en la Seu Electrònica usant el codi CSV següent:

URL (adreça en Internet) de la Seu Electrònica: https://sindicom.sedipualba.es/

Codi Segur de Verificació (CSV): KUAA YCVP W7J7 YYW3 U3UJ

En aquesta adreça podeu obtenir més informació tècnica sobre el procés de firma, així com descarregar les firmes i els segells en format XAdES corresponents.

Resum de firmes i/o segells electrònics d'aquest document

Empremta del document per a la persona firmant	Text de la firma	Dades addicionals de la firma
	Vicent Cucarella Tormo Síndic Major	Firma electrònica - ACCV - 15/09/22 07:44 VICENT CUCARELLA TORMO